

Regular Patent Application (RPA)

of

Kevin Kawakita

for

DIGITAL MEDIA DISTRIBUTION

CRYPTOGRAPHY USING

MEDIA TICKET SMART CARDS

Revision 3.00

Presented to the United States

Patent Office

December 2003

TITLE:

Digital media distribution cryptography using media ticket smart cards.

PATENT CLASS:

Process patent in the system of computer architectures and public key cryptography class.

PATENT SUBCLASS:

Public key cryptography architectures for commercial digital media distribution.

REFERENCES:

US PATENT LITERATURE:

[REF 10] Registered US Patent No. 6,367,019 Ansell, Steven T, et. al, et. Schneier, Bruce, "Copy Security for Portable Music Players," also called the "Schneier portable music patent".

[REF 300] Registered US Patent No. 5,315,658 (Micali Key Escrow)

[REF 304] Registered US Patent No. 5,276,737 (Micali Key Escrow)

[REF 308] Registered US Patent No. 5,231,668 (David Kravitz for the DSA authentication algorithm)

[REF 312] Registered US Patent No. 4,995,082 (Schnorr signature algorithm)

[REF 316] Registered US Patent No. 4,405,829 (Rivest, Shamir, Adleman, the RSA public key encryption algorithm)

[REF 320] Registered US Patent No. 4,200,770 (Diffie, Hellman public key exchange algorithm)

FOREIGN PATENT LITERATURE:

NON-PATENT REFERENCED PUBLICATIONS:

[REF 400] Schneier, Bruce, Applied Cryptography, 2nd Edition, John Wiley & Sons, Inc., New York, 1996, 758 pp's.

[REF 500] Recording Industry Association of America (RIAA), "The Secure Digital Music Initiative (SDMI)", www.sdmi.org, TBD pp's.

[REF 502] Recording Industry Association of America (RIAA), "The Recording Industry Association of America (RIAA)", www.riaa.com.

BACKGROUND - Field of Invention:

A preferred embodiment of the invention of a new type of public key cryptography architecture is introduced for internet "downloaded" central distribution of custom encrypted digital media over a prior art customer personal computer (PC) with attached physical media drives with physical, portable media and also attached media ticket smart card readers holding media ticket smart cards which portable media is manually transferred or "footprint downloaded" along with the physical digital media for playing upon a new type of cryptographic media player [REF 108] having a built-in media ticket smart card reader. The portable media may also come directly from the retail store.

A 1st alternative embodiment of the invention uses custom encrypted high definition "big screen" television (HDTV) and standard definition television (SDTV) digital transmitted MPEG II compressed digital signals to transfer the media to home television sets over the airwaves, transmitted over cable systems using fast, digital, cable broadband modems, transmitted over the phone system using fast, digital, asymmetric digital subscriber line (ADSL) broadband modems, transmitted over direct broadcast satellite (DBS) systems, transmitted over "wireless Ethernet" Institute for Electrical and Electronic Engineers Standard (IEEE) 802.11c (100 Mega bits/second) signals, and also transmitted over physical transfer channels using entertainment store purchase of digital versatile disks (DVD) pre-programmed with

digital media. The customer's unique media ticket smart card with custom play codes and play counts must be programmed over a separate internet based personal computer (PC) system with an attached media ticket smart card reader. The relevant television must have a special cryptographic set-top box. A relevant digital versatile disk (DVD) player for custom cryptographic media must have a built-in media ticket smart card reader with the proper media ticket smart card inserted.

A 2nd alternative embodiment of the invention uses digital versatile disk (DVD) as a physical transfer channel to distribute commercial movies to movie theaters with the customer/theater owner's unique media ticket smart card programmed with custom play codes and play counts over a separate internet based personal computer (PC) system with a media ticket smart card reader. The digital, micro machine module (MMM) based movie projector with up to 30-channel theater-type sound system and even multi-dimensional sensory digital outputs such as seat vibration units, seat temperature units, and olfactory units must have a built-in media ticket smart card reader with the proper media ticket smart card inserted.

This invention relates to a specific new type of process or system of implementing a public key cryptography architecture implementing a system of processes with both prior art hardware, software, protocols, and cryptology algorithms and the inventor's new art cross-referenced systems components.

The prior art hardware components and new art hardware components based upon the inventor's cross-referenced patents (see CROSS-REFERENCES TO MY RELATED PATENTED INVENTIONS Section), or else based upon public domain published research from the inventor's technical journal articles, or else based upon the inventor's already published US patent material without relevant subject patent filing within expiration of the US Patent Office's (USPTO's) 'one year publication rule' for any form of public publication or public dissemination of information are:

media ticket smart cards (880) (prior art),

media ticket smart card readers (900) attached to standard

personal computers (PC's) (820) using universal serial bus (USB) cables (prior art),

(optional) bio-identification digital fingerprint readers attached to the media ticket smart card readers (used instead of a passphrase/passcode entered into a toggle field with display for customer identification),

local area networks (LAN's) (924) (prior art),

internet protocol wide area networks (IP-WAN's) (928) (prior art),

commercial personal computers (PC's) used as clients (820)
(prior art),

world wide web (WWW) servers (824) (prior art),

cryptographic media players (700, 720, 1000, 1004) with built-in media ticket smart card readers and media drives for different format commercial medias, patent pending [REF 508],

cryptographic digital signal processors (C-DSP's) (932) [REF 500] used inside of cryptographic media players (700, 720, 1000, 1004) [REF 508], [REF 510], and other open systems computing components.

The software components involved are:

high security server operating systems (HS-OS's) (920) (prior art),

cryptographic algorithms (prior art), and

cryptographic protocols (prior art).

The systemwide goals of this invention is to provide a new method or process of using existing hardware components to provide centralized web server support and worldwide computer industry and internet standards and processes for:

1). Public key cryptography and private key cryptography in a hybrid use called hybrid key cryptography specifically tailored to the application of world wide web (WWW) centralized media server (WWW server) based internet distribution and download to prior art customer personal computers (PC's) of custom encrypted, commercial digital media limited to media which can be real-time, custom decrypted upon a specialized cryptographic media player [REF 500] (e.g. digital movies, digital music, electronic newspapers, and electronic books).

The internet download occurs from web media servers to customer's commercial prior art personal computers (PC's) containing drives holding digital physical media consisting of in example media being digital versatile disks read write (DVD-RW (R), DVD+RW (R)), compact disk record once media (CD-R), or flash type solid state memory cards (FLASH (R)).

The internet download occurs from web media servers to customer's commercial prior art personal computers (PC's) containing built-in media ticket smart card readers with the customer's inserted media ticket smart card which controls media replays.

A cryptographic media player with a built-in media ticket smart card reader and built-in media drive to play the custom encrypted media.

Also in a separate application called the 1st alternative embodiment, the custom encrypted digital media can be broadcast as

high definition television (HDTV) and standard definition television (SDTV) signals to an "over the airwave" set-top box on top of a digital television monitor or else a set-top box built inside of a home digital television. The "over the airwaves" set-top box will be a cryptographic media player with a built-in media ticket smart card reader to control media replays. An external or built-in digital versatile disk (DVD-RW (R) or DVD+RW (R)) drive or smart digital recorder will digitally record the custom "cipher text" or pre-encrypted medium. Also in the 1st alternative embodiment, the custom encrypted digital media can be transmitted over a fast broadband cable line to an over the television monitor cable set-top broadband cable modem box or over a fast asymmetric digital subscriber phone line (ADSL) to a fast broadband ADSL set-top box. The direct broadcast satellite (DBS) service (e.g. Hughes DSS (R), Echostar (R)) set-top box can also receive the same format custom "cipher text" or pre-encrypted HDTV/SDTV signals if it uses a cryptographic digital signal processing (C-DSP) unit. The set-top box or built in set-top box is a cryptographic media player able to control media replays through decryptions using the media ticket smart card. The cable modem or ADSL modem set-top boxes (with a return channel) can even have fully interactive digital electronic television guide information and future recording customer instruction using a simple spreadsheet or matrix type of graphical user interface (GUI) included for removal and display on the digital television monitor's picture in a picture (PIP) screen.

In a 2nd alternative embodiment of a movie theater application, a special movie, cryptographic media player (patent pending) [REF 108] with built-in media ticket smart card reader to control media replays will exist for commercial movie distribution to movie theaters of two disks per intermission interval for movie content plus an additional disk for local advertising, custom encrypted digital versatile disks read/write (DVD-RW, DVD+RW). This cryptographic media player will be integrated with a micro-mirror machine module (MMM) for digital movie theater color projection systems. The movie theater may also have an up to 30-channel theater type sound system. Future units will even have olfactory units, seat vibration units, and automatic theater light and drapery control. Digital versatile disk read/write (DVD-RW (R) or DVD+RW (R)) consists of 4.9 Giga bytes (4.9 thousand Mega bytes)/disk single sided and single layer. Greater capacity can be had using double sided and double layer digital versatile disks (DVD-RW (R) or DVD+RW (R)) for up to 20 Giga bytes (20 thousand Mega bytes)/disk of digital storage. Low quality, color, audio (2-channel)/video compressed digital MPEG IV is recorded at only 3 Mega bits/second or about 0.37 Mega bytes/second. Higher resolution MPEG IV can be recorded at 3 Mega bytes/second. Even the high resolution MPEG IV recording rate allows recording of up to 6,667 seconds or 1.85 hours per double sided and double layer digital versatile disk of very high quality MPEG IV compressed audio (2-channel)/video. A second double sided and double layer digital versatile disk read/write (DVD-RW, DVD+RW) drive can simultaneously read in additional audio channels for up to 30-

channel Dolby (R) types of theater sound systems. Digital versatile disk (DVD), concert quality sound is left uncompressed and recorded at a 44 Kilo Hertz rate with 16-bits/sample or 2 bytes/sample or a 88 Kilo bytes/second/channel data recording rate neglecting an extra 10% for error detection and error correction parity coding. 30 Dolby (R) channels takes a total of 2640 Kilo bytes/second or about 2.7 Mega bytes/second.

The second disk will even have spare capacity for additional future special effects in n-dimensions such as seat vibration unit effect track recordings, olfactory (smell emitter) track recordings, automatic theater light and drapery controls, nationwide and local theater commercial tracks, public service messages, etc.

The separate MPEG X audio stream and MPEG X video streams can be correlated with the MPEG IV "presentation time stamps (PTS)" and MPEG IV "system clock reference (SCR)" which is the initialization setting for a target system's hardware based digital timer. The session key hardware decrypted MPEG IV de-compressed digital output can be used to drive a micro-mirror machine module (MMM) for sharp, ultra-bright, theater type projection systems.

Two additional digital versatile disk read/write (DVD-RW (R), DVD+RW (R)) can be inserted after intermission for up to 3.7 hour theater presentations.

This custom encrypted physical digital media can be customer personal computer (PC) copied an indefinite number of times for

legal copyright law personal use and archiving and in case of lost, stolen, defective, or disputed media ownership called "fair use". This media is useless without the matching crypto keys or "play codes" and "play counts" in the customer's media ticket smart card. The matching customer "play codes" and "play counts" in the customer's media ticket smart card can be stored in a back-up card in case the media ticket smart card is lost, stolen, defective, or of disputed legal ownership. The registered customer can always get a new media ticket smart card from the public key distribution authority in case of a lost, stolen, defective, or disputed legal ownership media ticket smart card.

The custom encrypted digital media can be entirely sold or given away by physical digital media copying on a personal computer in something called legal "first use." The physical media is useless without transfer of the crypto keys or "play codes" and "play counts" from the customer's media ticket smart card to the buyer's media ticket smart card. The custom encrypted media cannot be played without a matching programmed media ticket smart card inserted into a cryptographic media player [REF 108]. The matching customer "play codes" and "play counts" in the customer's media ticket smart card can be stored in a back-up card in case the media ticket smart card is lost, stolen, defective, or of disputed legal ownership which may in turn be illegally sold or given away. The registered customer can always use a cryptographic media player to legally transfer the crypto keys in his own media ticket smart

card to the buyer's media ticket smart card with subsequent registration over an Internet connected personal computer.

Transfer of cryptographic keys called "play codes (encrypted session keys or one-time secret keys)" and "play counts (accounting counts of number of media decryptions legally allowed)" from one person's media ticket smart card to a backup media ticket smart card may be required for legal "fair use" back-up. Transfer of cryptographic keys for a registered customer from the public key distribution authority to a newly minted media ticket smart card may be required to replace a lost, stolen, defective, or disputed legal ownership media ticket smart card. Transfer of cryptographic keys from one person's media ticket smart card to another person's media ticket smart card may be required for legal "first use" transfer.

2). Internet download of cryptographic keys being play codes (session keys or one-time secret keys) and also play counts (paid for accounting numbers of plays also known as custom decryption counts, -1 for an infinite number of plays, or else allowance of free trial plays) occurs to a media ticket smart card. Before a media play also called a decryption, the play counts are decremented on the media ticket smart card by the cryptographic media player [REF 108].

3). Internet update of play code (session keys or 1-time secret keys) and play counts (paid for plays or counts of free trial

plays) held by a particular customer's personal media ticket smart card inserted into a built-in media ticket smart card reader on the customer's world wide web connected personal computer.

4). Physical transfer of custom encrypted digital media and a programmed media ticket smart card from the customer's personal computer (PC) to a cryptographic media player [REF 508] (e.g. cryptographic "MP3" music player where MP3 stands for Moving Picture Electronics Group standards I audio layer 3 (MP3) (audio only) compressed digital signals, cryptographic electronic book readers, cryptographic digital versatile disk (DVD) home movie players, cryptographic digital versatile disk (DVD) theater movie players containing physical digital media drives and a built-in media ticket smart card reader).

5). If play counts (counts of paid for plays or counts of free trial plays also known as custom decryption counts) contained on a media ticket smart card are greater than one, it is decremented and restored on the media ticket smart card. The play code (a session key also called a one time secret key) on the media ticket smart card is retrieved into the cryptographic media player's [REF 508] cryptographic digital signal processor (C-DSP) having tamper resistant non-volatile electrically erasable programmable read only memory (TNV-EEPROM) [REF 500]. The media ticket smart card can then be removed from the cryptographic media player [REF 508] for wallet storage or left in place. The custom encrypted digital media limited to real-time decrypted digital music, digital movies,

electronic books (e-books), and electronic newspapers is then played upon the cryptographic media player [REF 508].

6). Non-copyrighted commercial material and home-made material which is never custom, encrypted may be "played" by the cryptographic media player in non-encrypted form an unlimited number of times.

7). Full compliance with the US Copyright law in terms of legal "fair use" which is one to two copies of US Copyrighted material for archiving and records storage. "Fair Use" allows for a back-up copy in case of accidental damage, theft, natural disaster such as fire, flooding, storms, allows for disputed legal ownership (as any divorced person will support), also one or two convenience copies at different locations used by the same legal owner. A home copy and a portable vehicle copy is the marketing minimum requirement, but, not the legal requirement.

Full compliance with legal "first use" of US Copyrighted material which is the legal owner's right to sell or entirely give away the material in legal ownership transfer to another legal owner.

The standards used are proposed industry wide standards which will hopefully progress from proprietary de facto standards (accepted by widespread commercial use after market introduction by one corporation), into industry standards set by the US Recording Industry

Association of America's (RIAA's) Secure Digital Music Initiative (SDMI), US National Association of Broadcasters (NAB), the Electronic Industry Association (EIA), and then to nationally standardized bodies such as American National Standards Institute (ANSI), and international standards bodies such as the International Telegraphy Union (ITU). The US Federal Communications Commission (FCC) may be involved in US jurisdictional legal regulation of US airspace, US cable, and US phone systems.

BACKGROUND - CROSS-REFERENCE TO MY RELATED PATENTED INVENTIONS:

[REF 500] Future US Provisional Patent Application No. TBD, Filing Date TBD, Filed by Kevin Kawakita, is called "A Cryptographic Digital Signal Processor (C-DSP) Integrated Circuit." This utility patent adds a superset of functionality to a prior art digital signal processor (DSP) for the functionality of built-in cryptographic key storage, and dedicated hardware circuitry for 'streaming cryptographic media' processing at a low rate or at a high rate depending upon specific target commercial application. The silicon compiler added circuitry of Reed-Solomon (RS) parity coding will help with fast hardware error detection and correction important for both stream cipher and block cipher chaining modes of cipher data as well as prior art encrypt key 1, decrypt key 2, encrypt key 2 mode called 'triple key encryption (3-key) mode.' The silicon compiler added circuitry of fast hardware secret key encryption/ decryption with 'play-back only portable' models only needing decryption can use any prior art encryption standard such as very bit-manipulative (inefficient on byte oriented computers) IBM's patented Data Encryption Standard (DES) in any of several stream cipher or block chaining modes and also prior art triple mode (3-DES). On chip support for public key encryption will include support for the multiplication of two very large integer numbers using the binary square and multiply method. On chip support for session key (one-time secret key) use will be a true electronic noise random number generator. This describes a standard digital signal processor (DSP)

integrated circuit (IC) dedicated to fast processing of fixed point arrays of numbers for uses mostly in low-rate digital decompression of 'canned or pre-recorded' audio commercial music. Possible uses for low rate digital still photographic compression (JPEG I or JPEG 2000 algorithms) which will require DES encryption capabilities for secrecy and message digest cipher algorithms for data integrity. Built-in peripheral input/output (I/O) bus support gives access to 'wiretappable ('red')' computer buses. The low rate of fast fixed point array digital signal processing can handle decompression of digital audio (e.g. MP3, fast-wavelet, Advanced Audio CODEC (AAC (R))) and compression of digital still pictures (e.g. JPEG-1 or JPEG-2000) but not the high rates of full-motion decompression of digital audio/video (e.g. MPEG IV or fast wavelet compression audio/video). Audio/video compressed digital data as in MPEG IV has on-chip silicon compiler MPEG IV circuitry in either full digital compression/decompression (CODEC) mode, or else in 'canned data' or 'play-back only mode' support for digital decompression only (1/ 2 CODEC) mode. The TNV-EEPROM memory is for the secure storage of cryptographic keys which are 'pass-thru encryption' transferred into the chip over wiretappable ('red') or open computer buses. The cryptographic chip has built-in impedance monitoring circuitry to detect 'pin-probers' with smart tamper detection and the erasure of cryptographic memory upon such tamper detection.

[REF 508] Future US Provisional Patent Application No. TBD, Filing Date TBD, Filed by Kevin Kawakita, "A Cryptographic Portable Music Media Player With Built-in Media Ticket Smart Card Reader and Physical Media Drive," which may be put into the public domain knowledge. This device uses a crypto-digital signal processor (C-DSP) inside of a standard digital compressed music (e.g. Moving Picture Electronics Group Audio Layer 3 abbreviated to "MP3") audio only portable music player. The device has a built-in smart card reader connected by universal serial bus (USB) to the crypto-digital signal processor (C-DSP) for the pass-thru encrypted transfer of cryptographic keys held in the smart card used as a portable vault. The open or wiretappable ("red") computer bus must have pass-thru encryption with sequence numbers used on all transfers to avoid the known hacker attack called a 'recorded replay attack' in which a digital recorder simply taps off the bus data and re-uses it without ever needing to decrypt the pass-thru encryption. The medium can be in MPEG IV Level S1/E1 'cipher-text' format introduced in the inventor's cross-referenced patent application.

[REF 510] Future US Provisional Patent Application No. TBD, Filing Date TBD, Filed by Kevin Kawakita, "A Cryptographic Portable Audio/Video Media Player With Built-in Media Ticket Smart Card Reader and Physical Media Drive," which may be put into the public domain knowledge. This device for the 'playing' of 'streaming cipher-text commercially canned audio/video' or the error detection, decryption, and decompression of 'digitally compressed, digitally custom encrypted, and digitally error detected canned audio/video (e.g. the 'cipher text' format proposed in the inventor's cross-referenced invention called MPEG IV Level S1/E1)' uses a custom cryptographic chip-set architecture involving:

- 1) a crypto-micro-controller (C-uP) with built-in tamper resistant non-volatile read only memory (TNV-EEPROM) for cryptographic key storage.

- 2). silicon compiler library functions for hardware error detection and correction in the form of Reed-Solomon (RS) decoding of 'canned data'.

- 3). a silicon compiler library function giving hardware secret key decryption only perhaps using IBM's patented Data Encryption Standard (DES) in several prior art modes.

- 4). a silicon compiler function giving circuitry for Moving Picture Electronics Group X (MPEG X) digital de-compression only (1/ 2

CODEC), which fully error detected, decrypted, and decompressed digital data is used internal to a 'set-top box' for processing either prior art MPEG X compressed digital data or the new with this invention 'Moving Picture Electronics Group Level S1/E1' which is 'cipher text' streaming digital media.

The device has impedance monitoring on the chip wire meshes and also on the chip-set buses for tamper detection and subsequent erasure of any on-chip cryptographic memories. The device has a built-in smart card reader connected by universal serial bus (USB) to the crypto-digital signal processor for the pass-thru encrypted transfer of cryptographic keys held in the smart card used as a portable vault. The C-DSP can distribute keys from its own crypto-memory to other chips in the chip set in pass-thru encrypted form with sequence numbers. The open or wiretappable ("red") computer buses must have pass-thru encryption with sequence numbers used on all transfers to avoid the known hacker attack called a 'recorded replay attack' in which a digital recorder simply taps off the bus data and re-uses it without ever needing to decrypt the pass-thru encryption.

[REF 512] US Patent Pending Application No. 09/999,589, Filing Date Nov. 15, 2001, Filed by Kevin Kawakita, "Crash Prevention Recorder (CPR)/Video Flight Data Recorder (V-FDR)/Cockpit Cabin Voice Recorder (CVR) for a Light Aircraft with an Add-on Option for Large Commercial Jets. This patent is a process patent which covers the aircraft use of a process of digital video flight data recording and a playback mechanism structure with efficient man-machine interface for both safety and entertainment audio/video which uses an entirely new type of extension to the Motion Picture Expert's Group IV (MPEG IV) in a cryptography "silhouette-like" hidden background scene cutting technique to very efficiently store both position data (global positioning system or GPS-stamps), attitude data (inertial reference unit or IRU-stamps), video channel data, available channel data, and electronic television guide like data for video channel selection and future program recording. This 'silhouette-like' technique can be used for interactive television guide data and audio/video channel identification with very low over-head. This new 'silhouette-like' process is used instead of the extremely high operating system overhead, very low data rate during low-motion audio video, prior art MPEG IV prescribed "user data extensions" which are custom specialized use additions to either the standard MPEG II audio stream or the separate MPEG IV video stream (e.g. close captioning for the hearing impaired, teletext, electronic television guide information). The new 'silhouette-like' technique is included in the inventor's definition of

MPEG IV Level S1/E1 digital data stream although this patent is a process patent for video flight data recording.

[REF 516] US Patent Pending Application No. TBD, Filing Date Nov. 13, 2003, Filed by Kevin Kawakita, "A Hybrid JPEG/MPEG Specialized Security Video Camera." This patent is a machine utility patent for very specialized all digital security audio/video camera originally intended for use with the inventor's above video flight data recorder invention but usable in any high security government or commercial application. A dedicated JPEG X silicon compiler function for circuitry and a separate dedicated MPEG X silicon compiler function for circuitry along with a characteristic two lenses with independent auto-focus and computer motion control modeling of moving suspects through electronic pan and tilt is implemented in hardware. This patent includes certain aspects of the author's proposed MPEG IV Level S1/E1 specialized compressed digital audio/video 'cipher-text' data stream including the high data rate MPEG X video stream, low data rate MPEG X audio stream, and occasional interspersed JPEG X hi-resolution digital still picture.

BACKGROUND - Discussion of Prior Art:

Prior Art Legal Environment

Previous to year 2002, internet based US and European digital media distribution architectures have fallen in violation of the US Copyright laws. Peer to peer architecture media distribution schemes (e.g. Napster (R), Gnutella (R), MP3 Dot Com (R), etc.) connect home personal computers to gather digital media directly from other home personal computers through a world wide web server based central addressing and database function. These services have allowed customers to distribute to other customers digitally compressed free music and free movies without authorized licensing or rightful payment to copyright owners. Music distribution companies alone due to the much shorter computer "download" time of compressed digital music (with current technology in y. 2002 about five minutes per compressed digital song vs. 2 hours per compressed digital movie) are losing a recently estimated 2-3 billion dollars a year in revenues in a worldwide music industry estimated at y. 2002 50 billion US dollars in revenue (about 4-6% of product sales). In y. 2002 due to the minimum 2 hour download time for a feature length movie even with compressed MPEG IV digital, Hollywood movie sales are not yet significantly impacted. A single "hit" Hollywood movie such as Titanic can have y. 2002 2 billion US dollars in total worldwide distribution theater, cable, home video rental, and home video sales out of worldwide total theatrical movie revenue of 100 billion dollars (neglecting an equal amount of revenue

from ancillary product or promotional item and souvenir item sales). Store credits by record sale and movie ticket credits by ticket sold allocating hundreds of millions of dollars per year in artist's royalties to recording and performing artists through royalty payments and residuals (re-play royalties) are way down.

This type of US copyrighted music (e.g. MP3 format digital music) illegal duplication and movie illegal duplication is a Federal Copyright © law violation. This legal decision was decided in the US vs. Napster case of year 2002 decided by Federal judge Marilyn Hall Patel in San Francisco Federal court. Napster has since the Federal court decision struggled with bankruptcy.

The US Copyright law allowed legal use of US Copyrighted material of one to two copies for personal use anywhere (e.g. one copy for home use and one copy for automobile use) and archiving for record keeping purposes and emergency back-up purposes (e.g. fire, flood, theft, natural disaster, etc.) which is legally called "fair use" and is not a US copyright violation.

The US copyright law also allows something called "first use" of purchased copyrighted media which is the right to sell the media or transfer legal ownership in entirety to another person. Many existing digital copy protection mechanisms do not allow for both legal "fair use" and legal "first use."

Non-copyrighted, home-made material can be copied by the customer an unlimited number of times and is usually not under US Copyright law

unless the home-owner © marks and registers a copy for US Copyright protection.

A legal form of electronic distribution of digital music is desperately needed by the music and movie industries to stop rampant piracy of perfect digital masters which can be duplicated ad infinitum in digital to digital copying without distortions, losses, or degradations. The method should also allow personal archiving or "fair use" of one to two copies. Especially desired from a marketing viewpoint only is one copy for home use and one copy for automobile or portable use by the same person. The production of non-copyrighted, home-made material should be copyable an unlimited number of times. The method should also allow "first use" or the right of the legal owner to completely sell or transfer legal ownership of the media in entirety.

Prior Art Discussion of

Cryptography

Cryptography has been mostly used in prior art at the government level for the dedicated purpose of highly secure government and military applications. The intent of cryptography was nearly absolute secrecy between two communicating parties under the current state of technological development. This is called strong cryptography. This cryptography will always be needed at the highest levels of government and the military through highly classified, US National Security Agency (NSA) administered common commercial and military computer security (COMSEC) programs. Hardware schematics and algorithms are kept top secret and restricted to cleared personnel with a "need to know" with controlled access in physically contained US National Computer Security Center (NSCS) highest security rating A1 computer facilities and secured buildings.

Two forms of cryptography have developed, the older secret key cryptography (symmetric cryptography) and the newer (since the 1960's with Diffie-Hellman), called public key cryptography (asymmetric cryptography) (see US Patent No. 4,200,770). These are distinguished basically by the nature of the key exchange. Secret keys must be kept and exchanged in secret. This must be done through physical exchange of secret keys which also authenticates or identifies correct parties (exchanging slips of paper or whispering passwords in someone's ear) or

else secret keys can be exchanged through a secure, dedicated data channel linked only to correct parties (e.g. two-party trusted agent transports using a locked briefcase handcuffed to one agent, express mailed package or registered US mail).

Public keys in one popular algorithm known as RSA (R) have a public key pair associated with a unique private key pair with the public key pair being openly or publicly broadcast to any party to allow anyone the ability to encrypt secure messages. A public key pair is like a Cracker Jack (R) prize secret common encryption only ring which only encrypts messages. This encryption ring is available to any person wishing to use it for encrypting messages only. A private key pair is like a Cracker Jack (R) prize secret decryption only ring which only decrypts messages. This decryption ring is available only to one person wishing to decrypt messages encrypted by the other rings.

A public key pair is also like a treasure chest key which only unlocks the left side of a divided, two sided and two lidded treasure chest which also has a partition down the inside middle of the treasure chest with a letter slot through which to place a secret letter. The public key pair is available to any passing party as it is hung on a nail on the outside of the left side of the treasure chest when not in use. The private key pair uniquely matched to the public key pair is kept secret and is treated just like a secret key, but, is not called a secret key to avoid confusion with secret key cryptography. The private key is used only by authorized parties for decryption of encrypted messages. The private key is also like a unique key which only unlocks the right half of the two sided and two lidded treasure

chest for only one person to pick up and read letters left for him. The right side key is only held by one person, hence its name of a private key. The single private key also allows unique authentication of the single private key holding party for a reverse right to left side letter exchange (like an exchange of photo identification or fingerprints). Since the right side treasure chest key is assumed to be held by only one person, only this one person can reverse deposit an answer letter through the center divider slot from the right side to the left side of the divided treasure chest where it is available on the left side by pushing a button inside the left side of the box. This reverse process is called a private key authentication.

Instead of a divided treasure chest with two lids separately locked by two different keys, a similar analogy can be made using a house with only two doors, a single, private key, for a back door used only by the house's owner. The front door of the house has a public key left on a nail outside of the front of the house for anyone's use. The front door of the house opens to a closed atrium with a letter slot for anyone to drop a letter off meant for the single owner of the house. This process is like public key encryption. A push button in the closed front atrium will drop a letter down for the front door visitor which is guaranteed as coming from the house's owner, who alone has access to the back door of the house. This process is like private key authentication.

The private key pair is almost mathematically impossible to derive from the public key pair alone. Given the private key pair, the public key pair is publicly known, so, all crypto information is known.

e.g. RSA public key cryptography algorithm (see REFERENCES [REF 5]). Other algorithms work in a similar manner with a public part and a private part, but, may not require key pairs (see Diffie-Hellman public key exchange cryptography [REF 6] which does not do authentication).

Secret and private key administration is an important cryptography concept. Whoever holds the secret keys or private keys controls or administers the data as no one else can decrypt and read it or authorize data transactions. This is just like possessing a house key which gives access to a house. Only responsible and authorized parties should have a copy of any keys, just like possession of a house key. You don't want to trust your house key to a stranger or a burglar.

A key recovery process must be done by organizations who do not administer the secret or private keys or by the key's owner if a key is lost in order to decrypt data. This is just like entrusting your house key to a trusted neighbor. Key escrow also allows third parties to legitimately or illegitimately enter your house. The police can obtain a court ordered search warrant upon your neighbor to surrender your house key to search your house. Alternately if your neighbor is a moonlighting burglar, he can illegally enter your house and rob you. Hopefully, crypto key recovery is done through a lawful process involving the court system, otherwise, an illegal data wiretapping

process occurs which is like breaking and entering a house with stolen keys.

Key recovery is facilitated by the current concept of key escrow. Key escrow is the term for depositing a secret or private key copy with a trusted third party for key recovery. This is just like a house key copy which is left with a trusted friend or relative. [REF 400].

Key recovery is enhanced by several techniques. Key splitting is the term for breaking a secret or private key into two or more pieces such as a front half and a back half of a house key which can be left in key escrow with different parties, so, that all pieces must be "welded" back together or joined before data can be decrypted (or in our house case before a house can be entered). A specific embodiment of key splitting is discussed in US Patents No.'s 5,315,658 (Micali key escrow for Diffie-Hellman key exchange and also for RSA public key algorithm) and registered US patent No. 5,276,737 (Micali key escrow fixing a hole called a 'subliminal channel' in Diffie-Hellman key exchange). These two patents establish the technology known as "fair and fail-safe key escrow." The interesting 'key escrow verification' property of Micali key escrow is that a party who holds only the front half of a split key can verify that another party holds the correct and matching back half of the split key without giving away the key's functional equivalent to a metal keys ridge pattern to either party. The split keys can be verified without full key disclosure to any one party. [REF 400].

A more advanced method of cryptographic split key recovery among lets say among five parties is called 'majority voting' or else a 'thresh-hold scheme' by a prior art method such as Blum Blum Schub (BBS algorithm) for unique pseudo-random crypto key generation which furthermore requires in this example any three out of five parties to collaborate in order to piece together a working split key. This maximizes the chances of key recovery in case of a disaster scenario for any one party, but, increases the chances of collusion by any three out of five parties to illegally leak out key data. A '(m,n) threshold scheme with verification' allows the example (3,5) parties to verify their own entire split key escrow database without any single party obtaining a citizen/customer's single full key. [REF 400].

Any national commercial use federated split key escrow system should be based upon US National Computer Security Center (NCSC) 'orangebook' rated C3 or higher secure, physically isolated (non-Internet connected) crypto key databases. Any key transport out of these key escrow centers in the form of personal computer (PC) relational databases should be done by authorized paperwork initially with 'warm-blooded' hand signed with identification and eventually with strict bio-identification smart cards with the use of smart split key escrow cards used as portable cryptographic key vaults. Without strong Federal anti-espionage/interoperability laws and Federal licensing with criminal background influence upon management background checks, the key escrow databases will be money and power corrupted by 1% evil key escrow agents, with moderate Federal law 1/10% of 1% agents (1/1,000) will be corrupted, and even with strong Federal licensing insuring

anti-espionage/interoperability laws 1% of 1% (1/10,000) of the key escrow databases will be subject to money and power corruption. The 'real-life' corruption can be handled by legal prosecution and by serial number identification of all crypto keys and split crypto key databases. The use of the split key escrow databases are entirely for legal purposes, for recovering lost or stolen cryptographic keys always with audit trailed presentation of citizen/customer identification, for court ordered recovery of disputed data, and for court ordered wiretap access. The law enforcement use of key escrow even with smart card portable vault accessibility exposes all such accessed keys which must be regenerated and replaced with new crypto keys. [REF 400].

Key splitting produces dependent private keys. Having multiple dependent private keys is also functionally like having two or more keys held by different officers turned at the same time in order to launch a ballistic missile. Multiple dependent private keys is mechanically also just like putting different padlocks "in parallel" or all through the same latch of a treasure chest. All padlocks must be removed from the latch before the treasure chest can be opened. [REF 400].

Secret key cryptography is now used (year 2000) in electronic funds transfer (EFT) systems over mostly dedicated phone lines. Secret keys are held in computer dongles (parallel printer port pass-thru devices which look like plastic harmonicas) and physically exchanged once a month (hand carried or express mailed) and attached to personal computers before operation. Automatic teller machine (ATM) networks and credit card processing stations use secret key encrypted dedicated

leased phone lines and dedicated satellite links to reduce the risk of unauthorized access through physical security. Specific examples of secret key algorithms are DES (R), Triple-DES (R), RC4 (R), Safer, Safer Plus, Idea (R), and Skipjack (NSA classified). [REF 400].

Secret key cryptography is now (year 2000) used in the internet for password computer access and password based electronic funds authentication and transfer with remote transaction processing computers.

A secret key authentication loop back is done which does not require exchange of the secret keys or passwords over the currently unsecured and open internet (like an old party phone line). Instead, a random, clear-text message is chosen by sending party A and exchanged with receiving party B while having party B send-back a pseudorandom number value which can be used to verify an authenticated two-way looped back data link. Party A puts the randomly chosen, clear-text message through a standard message authentication cipher (MAC) which is a one-way hash function or message digest cipher (MDC) with a secret key. The message authentication cipher produces a message authentication cipher code (MAC Code) or pseudo-random fixed bit length number sometimes called a "hash code". Party A then sends the randomly chosen clear text message to Party B. Party B independently uses the standard message authentication cipher (MAC) with his own secret key copy upon the clear-text, received message to also produce a message authentication cipher code (MAC Code). Party B loops his own MAC code back to party A. Party A compares his own computed MAC code with the copy just received from party B. If they are the same, then the secret

keys for the MAC are the same on both sides and the parties are authenticated to each other. A hacker listening in on the communications line would receive the block of randomly chosen clear-text message and a MAC code from party B for the message. Nothing of value would be intercepted by the hacker. The hacker really wants to find out the secret keys used on both sides. No clues about the secret keys are obtainable from the exchange of information.

Secret key cryptography can be done in a software computer program. It is approximately 10 times faster done in a specialized hardware secret key encryption integrated circuit (e.g. IBM's Data Encryption Standard (DES) (R) integrated circuit) due to the fact that frequent cryptographic bit operations are not done efficiently on byte (8-bit) oriented machines [REF 400]. Hardware based cryptographic digital signal processing (C-DSP) integrated circuits have been designed or proposed [REF 500], with single chip integrated circuit (IC) devices such as:

- a wire-mesh intermetallic layer which detects pin probers breaking the wire mesh with an impedance reading triggering automatic erasure of the cryptographic memory,

- tamper resistant non-volatile electrically erasable programmable read only memory (TNV-EEPROM) (secure cryptographic memory),

- digital signal processing (DSP) functions supporting special cryptographic hardware functions such as large integer to large integer exponentiation by the binary square and multiply method which support several public key algorithms:

e.g. cipher text =

(plain text) exponent (Public Key modulo (integer n))),

plus built-in true random number generation from an
electronic source and also pseudo-random (PR) number generation,

built-in silicon compiler support for Reed-Solomon (RS)
parity error detection and correction very important for 'cipher-
text' block chaining modes in which a one-bit error is propagated
through the entire cipher block which adds about 10% extra parity
bits depending upon desired accuracy,

built-in silicon compiler support for hardware secret key
encryption/decryption such as IBM's patented Data Encryption
Standard (DES) which converts for example 'canned compressed
cipher-text' into 'plain text,'

built-in silicon compiler support for MPEG X and or JPEG X
algorithms for faster speed especially with high frame rate full
motion and full frame size audio/video data with 'canned
compressed cipher-text' needing only MPEG X decompression (1/ 2
CODEC function),

for use in some public key cryptography algorithms), true random number generation circuitry for cryptographic seed generation, either 2-channel (stereo) audio signals, supporting 5.1-channel theater type home sound systems with 5 audio channels of tweeter, mid-range, and woofer, and a 0.1 channel of dedicated woofer, supporting 30-channel (movie theater sound audio signals), supporting audio/video signals (DVD movie players), supporting electronic text (electronic book, or supporting electronic newspaper players),

artificial digital signal degradation algorithms can be executed before digital to analog converters (DAC's) create 1st generation analog signals with digital recorders to counter-signal piracy (lost information cannot be restored by hackers), another counter to 1st generation analog signal piracy using digital recorders are analog watermarking algorithms which introduce pseudo random (PR), hidden ("human imperceptible"), fine-line, noise patterns into digital audio or digital video which can be recognized for audit trail purposes after a suspected theft, also to counter 1st generation analog signal piracy of digital signals using digital video recorders videotaping premier movie showings, different types of algorithms can be used for analog watermarks of analog video data of subtle but visible to an observer, color, pseudo-random (PR) border background patterns on the displayed video such that a

"bootlegged" digital camcorder recording of a commercial 1st run movie can be identified back to the theatre, date, and time of showing of the movie. However, these background digital watermarkings can be digitally edited out with digital computers by a dedicated movie thief,

analog to digital converters (ADC's),

analog output line amplifiers (possibly with analog watermarking to mark Copyrighted material) which is off-chip due to high power needs and power line noise introduction.

A message digest cipher function (MDC) is like a message authentication cipher (MAC) in that it produces a fixed-bit output for any clear-text input, but, no secret key is needed. A MDC produces a fixed-bit, output message digest cipher code. Sometimes, a MDC is called a one-way hash function. A MDC is easy to go forwards, but, very difficult to go backwards. A message digest cipher (MDC) function is used for data integrity, to show that a plain-text message has not been truncated, lengthened, re-arranged, or altered.

A message digest cipher code (MDC code) can be secret key or private key encrypted to result in a digital signature. A digital signature confirms the integrity of the plain-text that is digitally signed and also the digital signature is almost impossible for anyone but the secret key or private key holder to create. A private key signed digital signature can be de-scrambled by anyone having the

matching public key, so, the digital signature is not encrypted text or "cipher text" with "scrambled text" being a better term. A secret key signed digital signature is "cipher text" as it can only be verified by a party with the common secret key.

Most companies will not exchange secret keys even over dedicated phone lines. This is against standard operating procedure (SOP) as wire-tapping hackers using "blue boxes" or illegal phone test frequency generating boxes can easily pick off unencrypted passwords. Exchange of secret keys and passwords is also done through the US Postal System more affectionately called "snail mail". Despite its slowness and occasional mis-delivery, the US Postal System is currently more physically secure, more legally protected through felony, mail tampering and mail privacy Federal laws, more tamper resistant, and through certified return receipt mail is totally legitimate as court admissible evidence. Today's e-mail and web commerce is inadmissible as court evidence without extensive eye-witness corroboration because it is too easily tampered with or totally falsified.

Public key cryptography is now (year 2000) used in the internet in limited form for secure electronic funds transfer and authentication (verification) of connected parties. Verisign (R) is a major vender of this commercial software which is embedded in web browser software in a form known as a "Secure Sockets Layer (SSL)". The web browser software is sent out by manufacturers (e.g. Microsoft (R)) in compact disk (CD) form already containing a public key generation algorithm almost universally using the 512-bit key RSA (R) algorithm and a secret key algorithm almost universally using the 56-bit key triple DES (3-DES) (R

) algorithm. In y. 2000, 56-bit with 8-bits parity Triple-DES (R) is the international electronic funds transfer (EFT) commercial standard used by the American Bankers Association which many other nations adopt which is roughly equivalent to a 168-bit secret key. Upon web installation, the RSA algorithm generates a unique, customer public key and private key pair which is secret key encrypted and embedded in the user's hard disk drive within an encrypted password file for later retrieval and secret key decryption. Specific examples of public key cryptography algorithms are Diffie-Hellman (R) key exchange, Schnorr-El Gamal encryption algorithm, RSA (R) encryption and authentication algorithm, DSA (R) authentication only algorithm, and the latest algorithm elliptic-curve algorithms reducing in some special cases to several subsets of Diffie-Hellman (R) and similar discrete logarithm algorithms.

The web browser will establish a "secure sockets layer (SSL)" with a common public key database held by a trusted third party (e.g. Verisign (R) Web database). The user's unique public key will be sent to and stored in the public key distribution web database for authenticated distribution to any interested party. The public key distribution authority is also called a certificate authority (CA) who acts as a trusted third party by passing out digital certificates or authenticated, digitally signed copies of people's public keys. An International Telegraphy Union (ITU) standard for public key certificate distribution has been developed called X.509.

The customer uses his web browser to connect up to a commercial vendor (such as a bank) who in turn contacts the trusted third party

public key web distribution database (e.g. Verisign (R)) for customer authentication to the bank and bank authentication to the customer. This is all done by the public key distribution authority delivering personally digitally signed public keys to all parties. The trusted third party acts like a go-between who sets up a blind date and assures "daters" that the other person is not a crook or serial mass murderer and rapist.

In public key cryptography terminology, the trusted third party is also called the public key distribution authority (PuKDA) or certificate authority (CA). The PuKDA is trusted by everyone and it passes out and publishes authenticated, digitally signed, public keys in the form of digital certificates to anyone who requests them for all entered parties. This process is called public key digital certificate distribution. Trusted third party servers are also technically called authentication servers. The trusted third party or certificate authority holds the public key database for community access and distributes digitally signed, public key certificates. These have an American National Standards Institute (ANSI) and International Telegraphy Union (ITU) standard called X.509 [REF 400].

Secure Sockets Layer (SSL) sounds good on paper until people realize that hackers simply have to use a remote Internet virus to plant a keyboard capture buffer to record all passphrases/passcodes and passwords including all log-on and computer account passwords. The keyboard capture buffer is accessed remotely over the Internet through Web cookies or else through virus altered victim e-mail operations. Once the hacker gets this data, any cryptographic keys (public

keys/private keys or secret keys) hidden upon hard disk drives can easily be remotely read over the Internet and decrypted. A cryptographic algorithm which would require 100 years of super-computer use to decrypt is completely by-passed using keyboard capture buffers. It is also only a matter of time before hackers figure out where on a hard disk the permanently stored and secret key or password encrypted cryptographic keys are stored (mixed with pseudo-random noise called 'salt'). A hacker program will automatically search out this hard disk location and give hackers the cryptographic keys. Secure Sockets Layer stand-alone is very insecure without hardware cryptographic memory storage (crypto-CPU's, crypto-DSP's) and crypto-keyboards used to pass-thru encrypt passphrases/passcodes over wiretappable or 'red' computer buses such as keyboard buses and micro-processor buses.

In y. 2002, a form of hybrid key cryptography is usually used in practice which combines public key cryptography and secret key cryptography. This is because public key cryptography is often 1000 times slower than secret key cryptography done all in hardware at comparable cryptographic security levels (256-bit public key/77 digit number vs. 64-bit secret key/19 digit number excluding parity bits) [REF 400]. This ratio is public key cryptography being about 100 times slower than secret key cryptography when everything is done in software [REF 400]. In hybrid key cryptography, public key cryptography is used for authenticating parties and exchanging one-time secret keys (session keys) used for secret key cryptography.

Phil Zimmerman's Pretty Good Privacy (R) is not an algorithm, but, a collection of known Freeware Foundation (R) public key encryption utility programs for personal computers which allow almost unlimited strong encryption capabilities. It uses several proven secret key and public key cryptography algorithms. It uses a flat (sometimes called direct) or else a non-government authorized "web of trust" public key infrastructure. This "tangled web of trust" is simply one local public key database trusting another local public key database which trusts another local public key database, etc. Pretty Good Privacy (R) is now widely available in the US for domestic use only [REF 400].

Foreign nations have no restrictions on public key cryptography use. Software packages are widely available in Europe and Asia for personal computer use. Many widely, published, non-classified journals such as "Crypto", university textbooks, and European and US Patent Office publications give different cryptography algorithms which are considered public information of which many are patented and licensable.

The benefits of cryptography are that various security functions and legal attributes can be restored to electronic commerce. Among these are:

- 1). authentication (like an exchange of picture ID's or thumbprints),

- 2). privacy (secrecy or confidentiality),
- 3). integrity (wholeness and non-tampering),
- 4). digital signatures (like cursive signatures and dating of documents),
- 5). non-repudiation (denial of a digital signature by the signing party),
- 6). authorization (like an exchange of handwritten signatures on written orders or agreements),
- 7). accessibility (restricting access to authorized users)
- 8). archiving (data record storage of digitally signed and dated documents),
- 9). audit trail (recordings of accessibility to data),
- 10). play codes and play counts (controlled access to electronic digital masters).
- 11). crypto key splitting and key escrow
- 12). crypto key architectures for key administration

Prior art electronic commerce is woefully lacking in these elements leading to a huge erosion of personal confidence and privacy, business confidence and privacy, secrecy in government, and weaknesses

in policing authority. Strong cryptography can prevent US Constitutional 4th Amendment violations (illegal government search and seizure) against private citizens and businesses. Strong cryptography can distribute the power of knowledge and information of the global internet and it can thwart the actions of a corrupted high level US government official such as a corrupted president or CIA or FBI director.

Thomas Jefferson said that any concentration of power will eventually be abused by a wicked or evil authority. Modern interpretation is that any concentration of knowledge, power, or authority will eventually be abused by a wicked or evil authority.

Other prior art approaches to this problem have been the ill-fated, NIST (US National Institute of Standards and Technology (NIST) formerly called the National Bureau of Standards) and US National Security Agency (NSA) reviewed Clipper chip using the classified, secret key, Skipjack algorithm. Retrospective analysis of the Clipper effort in the year 2000 by many experts shows that it was a good research effort which developed many key hardware technologies and opened up healthy public debate regarding important public policy cryptography issues [REF 400]. The program did not fail technologically, but, failed in terms of the US Constitution, it failed in international politics with other countries, and it also failed commercially because no one trusted the US NIST/NSA/CIA, and FBI with over-whelming power to wiretap any digital transaction in the entire world!!!! Clipper did not address key US Constitutional issues of protection of individual freedoms, a system of checks and balances, and

distribution of power. Clipper did not protect in any way foreign freedoms and liberties represented by sovereign foreign nations.

Clipper was part of a larger group of hardware projects called Capstone introduced by NIST and NSA in 1993. Clipper was meant only for embedded use in portable voice-only, digital phone modems. The phone modem had to be carried around for portability. The Capstone's Fortezza product was meant for digital data using stream cipher encryption in PC Cards (then called PCMCIA cards) the thick, credit card sized plug-in cards which could be put into shirt pockets and plugged into laptop computers for use on computer data [REF 400].

Clipper was a hardware integrated circuit (IC) based chip of secret design implementing the secret key, Skipjack algorithm. No public key cryptography was involved. Working chips were produced by VLSI (R) Corp of Sunnyvale, California and programmed by Mycotronix (R) Corporation of Torrance, California in a classified program. These chips were used in production AT&T voice modems. Speculation on the design frequently proposes a 32-bit micro-computer or programmable computer on a chip with built-in tamper resistant, non-volatile read only memory (TNV-EEPROM) for holding secret key and computer program storage. Alternately, the hardware has been proposed as consisting of a dedicated custom application specific integrated circuit (ASIC) doing Skipjack secret key hardware encryption and decryption combined with tamper resistant, non-volatile memory for secret key storage [REF 400].

The NIST proposed Clipper chip was proposed for use on both ends of every secure voice communication channel through the use of

dedicated modems containing the chip. Clipper was intended for secret key, voice encryption only (it ran the block cipher Skipjack algorithm only in output feedback mode (OFB) mode which converts the block cipher into a stream cipher). The secret keys were to be locked into the tamper resistant hardware for only one user or residence party having the crypto modem. Mobility was done through carrying the phone modems around while security came from keeping the modems locked up or in a secure physical building and rooms. The Clipper program used no public key cryptography algorithms, but, was entirely based upon secret key cryptography. Public key cryptography was added in later into the Capstone program. Clipper also had no session key or one-time secret key exchange algorithm (e.g. Diffie-Hellman key exchange) specified with the Clipper program, but, this was added later with the Capstone program. Clipper session key exchange was done with an assumed "out of band" protocol. See REFERENCES Section - Non-Patent Literature - [REF 400].

Only the FBI had the ability to wire-tap the Clipper's encrypted data and decrypt the data after capture or in mid-stream by retrieving split in two, secret keys held by encrypted serial number (a secure hash code) in key escrow by trusted third parties. The US Treasury Department was to hold the front-halves of the unique, secret keys and the US National Institute of Standards and Technology (NIST) was to hold the back-halves of the unique, secret keys. Both halves of one secret key were to be released from key escrow to the FBI only under court order for a certain key serial number. The homeowner or business

owner could also get a full key out of key escrow if his key was lost [REF 400].

The secure modem with a Clipper chip held a family key as well as the unique secret key. The family key was used by the modem to encrypt the modem's encrypted serial number. The family key as well was used to secret key encrypt a session key or one-time secret key used to encrypt the message. This resulting data was appended to the message stream in a classified format, data field called a law enforcement access field (LEAF) accessed by the common family key. The LEAF was restricted to authorized law enforcement use, it was not used for "in band" or inside the communications channel session key exchange by the two parties. How the two parties exchanged session keys was through an unspecified "out of band" or outside the communications channel secret key exchange protocol (e.g. Diffie-Hellman Key Exchange Protocol) [REF 400].

Law enforcement could legally with a special "cipher (encrypted) text wiretap" court order or even illegally without a court order (there were no technical restraints to stop such action) wiretap and record a Clipper encrypted phone message. This is like separating a needle in a sealed envelope from a haystack. To decrypt the message, law enforcement would still need the family key held in key escrow using key splitting between the FBI and US Justice Department which would assumably only be released with "probable cause" of a common crime submitted to a court for a court order. A Foreign Intelligence Surveillance Act of 1978 (FISA) wiretap only for "national security" cases would not need "probable cause" of a crime. The whole family key

would be needed for law enforcement to access the law enforcement access field (LEAF) header in the digital message which only contained session key data for legal law enforcement wiretapping [REF 400].

The LEAF format was classified, but, is widely believed to be just the result of the sending modem A using the common, family key embedded in the modem to encrypt a field having three things:

identification of secret, encrypted, modem serial number A,

secret key A encrypted session key A (a session key is just a secret key used for just one message)

secret key A encrypted tamper resistance field [REF 400].

Law enforcement would still need the whole, secret key A held in key escrow using key splitting between the US Treasury Department and the US National Institute of Standards and Technology (NIST). Law enforcement could use the whole, secret key A to decrypt the LEAF held session key (1-time secret key) which in turn could be used to decrypt the digital voice message attached to the LEAF [REF 400].

Law enforcement could legally with or without a court order wiretap an encrypted message through a "cipher text (encrypted text)" wiretap. This would be like separating a needle in a sealed envelope from a haystack. This technique used without a court order might be legally justified for FBI use on "highly suspicious people with proven associations to known, violent terrorists." The "cipher-text wiretap"

would be useless without eventually getting crypto keys from key escrow under a court order with "probable cause of a crime." A FISA wiretap under the Foreign Intelligence Surveillance Act of 1978 used only in "national security" cases would not need "probable cause" of a crime but a court order from the FISA 7 member panel of Federal judges appointed by the Chief Justice of the US Supreme Court. A court order would be obtained by showing to a Federal judge or local criminal court judge legal "probable cause" of a serious misdemeanor or felony. Law enforcement could then use the court order to obtain the key split, family key held in key escrow by the FBI and the US Justice Department [REF 400].

Law enforcement with a legal court order for a wiretap, could use the whole, family key to access or decrypt the LEAF. The decrypted LEAF would uniquely identify the modem producing it through the secret, encrypted, modem serial number A. Law enforcement could take the legal court order and the modem serial number A to both the US Treasury Department and the US National Institute of Standards and Technology (NIST) in order to obtain the key split secret key A held in key escrow [REF 400].

Law enforcement would now have a legal court order for a wiretap, a whole family key, and a whole secret key A. The secret key A could then be applied to the LEAF to obtain the decrypted session key or one-time secret key used for just one message. The session key could be used to decrypt any stored encrypted messages and any future encrypted messages [REF 400].

Law enforcement could finally use the decrypted session key to decrypt the voice digital message. Only the one-time secret key or session key was used to encrypt the message [REF 400].

Objections to the Clipper chip proposal were from many respected sources and very heated. With a secret hardware design and classified crypto algorithm plus secret NSA production and distribution of hardware, there was no way for civil libertarians, foreign governments, foreign scientists, academic scientists, and commercial scientists to check for "back doors" to prove that escrowed encryption was technically as well as legally supported in an honest manner. A "mole" or spy in the central, NIST (technically backed by the NSA) production apparatus, a bribed NIST (technically backed by the NSA) official unable to turn down a billion dollar deposit into an anonymous Swiss bank account, or even a politically coerced high NIST (technically backed by the NSA) official, would have access to whole keys before key escrow and could tamper with Clipper hardware or introduce rigged hardware chips [REF 400].

e.g. In example, rigged computer hardware chips have even been introduced by bribed Bally (R) employees into the highly secure production of Las Vegas electronic poker machines. The rigged poker machines were looted by "inside job" "swindle ring" customers who triggered artificial jackpots by placing planned token bets when known card sequences randomly showed up in order to trigger further planned bets placed upon subsequent programmed card sequences which

eventually led to artificial jackpots. The suspect machines were inspected and declared secure by a high level Las Vegas Gaming Commission official in charge of firmware validation and verification who was the mastermind of the entire swindle and main recipient of millions in dollars in cash, illegal gambling proceeds. The high level gaming official was eventually caught, tried, and convicted based upon the testimony of his low level accomplices.

With classified hardware, firmware, and crypto algorithm design, no independent party could verify if the Clipper hardware or Skipjack crypto algorithm were secure through open scrutiny. A secret backdoor could be intentionally put in the hardware by the NSA to by-pass key escrow. An accidental design or production flaw in the Clipper chip could easily be exploited by hackers to by-pass security. A secret backdoor could be intentionally put in the Skipjack algorithm by the NSA to by-pass key escrow such as by using an uneven key space or non-linear key space known only to NSA officials. The Skipjack algorithm could be vulnerable to some odd or newly discovered mathematical attack unknown to NSA officials, but, known to some Russian mathematicians and the Russian secret police [REF 400].

The key escrow process itself was criticized as being inadequate in that all escrow parties were in the executive branch of the US government under political pressure of the President of the United States [REF 400]. If this President happens to be Richard Nixon using Internal Revenue Service (IRS) tax records and surprise income tax

audits against political opponents, illegal breaking and entering, and illegal wiretapping devices planted by ex-CIA and ex-FBI agents, the US citizen and foreign governments are not too assured of security. The logical choice would have been to put the US Supreme Court and Federal courts in charge of half of the relevant keys to defend the US Constitution and Bill of Rights (especially the Fourth Amendment injunctions against illegal search and seizure), and a neutral legislative party such as the US Congress' General Accounting Office (GAO) otherwise known as the investigative arm of the US Congress in charge of the other half of the keys. This key escrow storage would have respected the three division of powers in the US Constitution, the executive branch, the judicial branch, and the legislative branch.

Foreign governments and foreign businesses did not trust the US key escrow process and were afraid of legal and illegal US government intrusion into their own government and business secrets. Foreign governments instituted their own strong encryption technologies free from the artificial key length and key escrow restraints of the NSA [REF 400].

If Clipper was compromised through security leaks or a single, crooked central key escrow employee, a corrupted government authority, foreign government, or anarchist hacker group could still undetectedly wiretap every single digital transaction and phone conversation in the entire world!!!! Civil libertarians, foreign businesses, foreign governments, and US business interests rigorously opposed its introduction [REF 400].

There were also technical complaints that the Clipper program was too rigid in that it did not support transportable keys (through dongles, Smart Cards, or PC Cards). Clipper did not support multiple crypto algorithms other than Skipjack. In the early 1990's, the prevailing commercial standard was 56-bit secret key, Triple-DES (3-DES) in Cipher Block Chaining (CBC) mode. Clipper hardware used in Capstone also did not support block cipher modes and only supported Output Feedback (OFB) stream-cipher mode although other modes could be used with the Skipjack algorithm [REF 400].

The public key cryptography algorithms supported for Capstone were Digital Signature Algorithm (DSA) for authentication of parties (who), Diffie-Hellman for Session Key (1-time secret key) exchange (what). Meanwhile in y. 1993 until currently in y. 2002 the de facto industry, worldwide public key cryptography standard was and still is 1024-bit key, proprietary RSA (R) algorithm. Clipper hardware used in Capstone also did not support block cipher modes and only supported Output FeedBack (OFB) stream-cipher mode although other modes could be used with the Skipjack algorithm. The PC cards used in Capstone with the Skipjack chip did very slow stream cipher encryption and natural mode block cipher encryption with the data stream fed in from the personal computer with a PC card reader [REF 400].

There were also legitimate complaints that a legal process of a court ordered wiretap would quickly expose or compromise whole, family keys to all involved parties. All modems using a certain family key

would have to be re-programmed to retain secrecy of the family key [REF 400].

All compromised modems from a legal wiretap with exposed unique serial numbers for the modem A from a legal wiretap would have to be re-programmed with new keys re-issued and re-key escrowed [REF 400].

There were legitimate complaints that the 16-bit (64 thousand possible combinations), unique, tamper resistance field which was put in to foil brute force, computer attacks upon the LEAF could be easily guessed through a computerized brute force hacker attack upon the LEAF. The brute forced LEAF could even work with a guessed, wrong tamper resistance checksum matching a guessed, wrong key in the field. The Clipper containing modems were initially programmed to simply ignore messages with bad tamper resistance field checksums. NSA's response to the weak LEAF complaint was to reset the Clipper modem after receiving 10 bad LEAFs possibly from a hacker which would force an inconvenient delay to the hacker. This would simply slow a hacker's automated computer key cracking program down while the hacker is off eating a pizza [REF 400]!!!!

A partially compromised LEAF would yield the encrypted modem serial number which would mean that all Internet or voice transactions with the "clear-text (unencrypted)", modem serial number A could then be parsed or isolated by hackers by decrypting the LEAF field of all desired messages for modem serial number A. A compromised, once-secret, modem serial number A could be used to bribe government officials into revealing a whole, secret key A. The secret key A could

be used to obtain the one-time, 80-bit, Session Key A (1-time secret key) from the LEAF of any message sent by the modem serial number A. This would compromise all messages sent by parties from modem A [REF 400].

At about the same time in 1994, NIST (with technical review and support from the NSA) also announced a larger group of crypto hardware projects called Capstone which also used the classified secret key Skipjack algorithm and escrowed storage of key split (like breaking a house key into a front half and a back half) secret keys (using Micali Key Escrow [REF 1]). These hardware and firmware initiatives supported a broader range of crypto issues including:

- 1). crypto key mobility through the PC Cards (PCMCIA cards).
- 2). key escrow using the Escrowed Encryption Standard (the same as for the Clipper chip),
- 3). public key cryptography authentication of parties using the Digital Signaturing Algorithm (DSA) algorithm (developed by the National Institute of Standards and Technology with NSA technical support),
- 4). public key cryptography exchange of secret keys and session keys (probably using Diffie-Hellman public key Exchange),
- 5). data integrity support through the secure hash algorithm (SHA),

6). a hardware large integer number exponentiation program for doing faster DSA public key authentication and Diffie-Hellman key exchange mathematics,

7). and a hardware true random number generator.

8). internet support through the generic, Mosaic program. Mosaic was the predecessor to both the Netscape Navigator (R) computer program and also Microsoft's Internet Explorer (R). Mosaic was developed at the Univ. of Illinois by a team including a lead graduate student researcher, Mr. Marc Andreessen, who copied the source code and improved it with venture capital money to form the original Netscape Navigator) [REF 400].

The Fortezza card (initially called the Tessera card, but, changed due to Copyright violations) was a member of project Capstone. It was a classified design PC card (PCMCIA) card which is a thick credit card sized electronic plug-in card for laptop computers which was used for stream cipher encryption by a laptop computer or desktop personal computer. Production cards were produced with Mycotronix (R) Corporation firmware and VLSI (R) Corporation hardware for US State Department and CIA field office use with lap-top computers hooked up to standard phone lines through standard modems [REF 400].

The Fortezza card probably had [REF 400]:

- 1). tamper resistant, non-volatile memory (TNV-EEPROM) for secure key storage,
- 2). a 32-bit embedded microprocessor or faster dedicated circuits for the Skipjack algorithm,
- 3). a random number generator circuit for generating session keys and also white noise used in some public key cryptography algorithms (e.g. El Gamal),
- 4). large integer number to large integer number exponentiation hardware for RSA and other public key cryptography,
- 5). static random access memory (SRAM), and
- 6). a PC (PCMCIA) card reader interface.

Capstone's firmware or embedded software did authentication of parties using DSA, Session Key (one-time use secret key) exchange probably using Diffie-Hellman, and then self-contained Session Key encryption of data using the classified Skipjack algorithm [REF 400].

The criticisms of Fortezza were the same as for Clipper. Added criticisms of Fortezza were that the card was too expensive at US \$25 retail vs. \$5 for a smart card and \$0.25 for a magnetic strip card. The card was too thick at 1/4" vs. credit card thickness for a smart

card. The internal to the card stream cipher encryption/decryption had to be fed-in from the personal computer with a PC Card reader and was too slow for a late 1980's era speculation regarding a classified program 18 MHz low cost embedded micro-controller or application specific integrated circuit vs. a 33 MHz Intel 486 used in comparable desktop systems of the time [REF 400].

Prior Art Discussion

on Smart Cards

Many US Patent and Trademark Office (USPTO) and European Patent Office (EPO) patents have already been issued for micro-controller based smart cards with non-volatile electronic memories for cryptographic key storage, identification numbers, bio-identification data, and cash debit amounts: smart cash cards and distribution systems, smart phone cards, and smart voting cards. Smart cards have been extensively used in Europe for over fifteen years.

Smart cards have progressed rapidly in Europe in commercial and government uses despite their high relative cost compared to magnetic strip cards used in the US due to the poor reliability phone systems (99% up-time) in Europe and the lack of central phone standards while the US has always enjoyed reliable telecommunications (99.999% up-time) and national phone standards. Magnetic strip cards cannot be used stand-alone while smart cards work well stand-alone.

Smart cards based upon optical memories which are thin transparent plastic strips holding laser beam readable digital data use optical technology similar to compact disks and digital versatile disks. The smart optical cards themselves are encoded with forward error correction which allows self-correcting data in redundant forms,

however, they are still prone to abrasion, and acid damage while being largely immune to electro-magnetic discharge (static) damage and water damage. The draw-back of these cards is the need for a smart optical card readers are expensive US \$20,000 per item which must connect up to a personal computer.

New forms of extremely secure and private smart card (212) based electronic cash cards, electronic banking debit cards, and electronic credit cards will be possible in the early 21st century. Internal debit and processing circuitry in the smart card (212) will allow some stand-alone operations without any form of remote connection for use in emergencies and areas with poor or no Internet access. The requirement for single point of failure survivable, full forward and backwards audit trail of all smart card financial transactions makes for extremely difficult cryptographic 'tracable electronic cash protocols.'

New technology is desperately needed to counter fraud in the old forms of pen, pencil, and paper hardcopy identifications, paper currency, and documents for government and commercial use.

e.g. This is especially true with the advent of cheap, personal computer (PC) based color scanners, easy to use color image editing software, and cheap color printers. Home use plastic lamination equipment with forged color identification (ID) produces authentic looking color ID badges at pennies on the dollar.

e.g. Color laser printers produce very passable US government currency used by teenagers for pocket money. The phony currency was once detected by color smudging with wet fingers and the rubbing of the paper which did not have the cloth feel of real US currency which is made out of linen. Recently, water-resistant ink-jet cartridges have been introduced which will produce water resistant cheap counterfeit money.

e.g. Billion dollar a year in revenue, foreign based and government condoned (Thailand and Taiwan), commercial forgery operations produce authentic looking US government ID such as state driver's licenses, social security cards, and certificates of live birth. Even three dimensional visible light laser holograms meant to counter forgeries are reproduced by million dollar commercial printing machines. The identities of deceased US citizens are used who were never reported in to the US Social Security Administration (SSA) or to individual state motor vehicle offices. This makes the identification cards good as the real thing in terms of by-passing fraud detection by computer databases.

e.g. Foreign US currency forgery rings operated by hostile foreign governments such as Iran under the late Ayatholla Khomeini produce such realistic US currency that the amounts are ignored by the US Treasury Department as being too costly to stop.

e.g. In the 1990's, billion dollar illegal cash revenue, commercial, printing operations using million dollar commercial printing presses, legally condoned by the Thai government and

headquartered in Thailand produce the latest computer visible light 3-dimensional holography, multi-layer, forged, US government identification cards including forged, US State Department passports, forged, passports from any foreign nation, forged US Social Security Cards using the Social Security Numbers of dead people (to pass through government computers if they have not yet been officially reported as deceased), forged, US California state driver's licenses using the state driver's license numbers of dead people, and forged, certificates of live birth in the US.

Forged California driver's licenses using the driver's license numbers of deceased people are so good that they routinely fool California Highway Patrol (CHP) Officers and even the California State Department of Motor Vehicles (DMV) mainframe computer.

e.g. Illegal aliens routinely purchase in Los Angeles' McArthur Park, the headquarters of the Hispanic illegal alien community from Mexico, Central, and South America, zip-lock bags of very high quality, Thai made, forged identification for \$500.

A typical \$500 zip-lock, bag will include three from the following list: a forged US State Department passport, a forged California driver's license, a forged Social Security Card, a forged certificate of live birth in the US. These documents are necessary to get a job in the US. The identities on the card are legal identities of dead people with the photo-

identifications updated to the imposter. The identification will pass through the state DMV computers and will fool a California Highway Patrol Officer.

California employers photocopy ID for their files for legal protection against hiring illegal aliens and the \$10,000 per alien fine, but, are usually loathe to question authenticity because of a shortage of stable (staying longer than six months after training), minimum wage workers. The few California employers who wish to comply with the law have no legal means to verify identification with the Social Security Administration (SSA) using photo ID.

[In y. 2002, the state of California has about 30-40 million state residents with estimates of as low as 33% up to 50% or a range of 13 million up to 20 million being illegal aliens in California mostly of Hispanic origin from Mexico, Central America, and South America. Migrant illegal alien farm workers pick 100% of the California agricultural harvest which is a 400 billion dollar state industry which provides much of the nation's seasonal speciality crops and winter vegetable crops. The illegal aliens facing unemployment and poverty in their countries of origin also willingly do the 'dirty work' in restaurants most of which will go bankrupt without illegal alien labor. In a robust 2 trillion dollar, hi-tech, California state economy which is 1/ 7th the entire y. 2003 US economy by Gross Domestic Product (GDP), illegal aliens take for long-term (longer than six months/job/employee) most of the minimum wage

"dirty work" jobs which Americans will not take such as field work, restaurant work, dish washers, fast food workers, gardeners, nanny's, and house-cleaners. This estimated 9 - 20 million illegal aliens in California is out of a y. 2000 US Census figure of 300 million US residents with as much as 30 - 37 million total US residents being of Hispanic descent, with an unknown number of illegal alien Hispanics, legal alien, and US citizen American-Hispanic ancestry. Y. 2002, US Department of Labor estimates give the total US Hispanic figure of 37 million residents of which as many as one-half or 18.5 million may be illegal aliens (the US Census figures are well known to undercount because illegal aliens and recent immigrants from repressive governments simply throw US Census forms out in the trash).

Many illegal aliens vote especially regarding illegal alien legislation and have 'swing voted' many local, state, and even US Congressional seat elections in California because there it is illegal under Californi^a law for voter registrars to do California state voter identification verification for US citizenship. Many illegal aliens drive without car insurance and with forged state driver's licenses which are so good that they fool the California Highway Patrol (CHP) and also the state Department of Motor Vehicle computer.

A few illegal aliens commit major crimes such as 1st degree murder and pre-meditated murder of a police officer and then disappear back into their home towns of Mexico, Central America,

and South America where they know that the Catholic dominated governments will not honor US extradition requests to any country or state with the death penalty. Identification of illegal alien criminal suspects is difficult due to forged legal alien status cards and forged state driver's licenses.]

The national security implications are obviously dangerous in an age of Al Kaida based terrorism because of: the prior art of basically undefendable US borders from illegal immigration, weak identification of immigrants to the US, 99% use of forged but legally passable identification used in applying for employment (to avoid the US \$10,000/illegal alien fine which is basically unenforcable due to forged driver's licenses and no photo-id for employer access), forged identification cards which are 99.9% passable used for employment, renting housing, buying airline tickets with 24-hour non-stop flights out of the US, forged but 99.9% passable identification of those applying for rental cars and apartments during high terrorist threat periods.

Microsoft (R) Corporation has launched a Windows 2000 smart card initiative for its Windows 2000 operating system (not yet released in January of 2001). This involves a standardized, embedded operating system contained inside smart cards. Not much has yet been published on this initiative (see <http://www.microsoft.com>).

Intel (R) Corporation has launched a cryptographic architecture in January of 1999. Not much published information exists on this initiative (see <http://www.intel.com>).

Prior Art Discussion on Digital

Electronic Masters

Digital masters for movies, music, video games, and computer programs are easily extracted from their current forms in digital versatile disks (DVD's), video tape, cassette tapes, and compact disks (CD's). An illegally obtained digital master is easy to illegally copy in digital to digital copying an unlimited number of times without degradation of the signal quality unlike an analog copy.

e.g. Taiwanese based commercial operations, legally pirate US, European, and Japanese music and movies for Taiwanese citizen use, since, Taiwan is not a member of the Bern international copyright convention. Taiwan is a notorious software, movie, music, and counterfeit brand-name product, piracy country which depends upon these revenues for hundreds of thousands of jobs.

The US and Europe are illegally flooded with hundred's of millions of dollars worth of Taiwanese produced, illegally made copies of DVD and VCR format movies, cassette tape and CD format music, CD format and ROM-pack format video games, and CD format computer software.

e.g. Napster (R) is a 1999 corporation creating peer-to-peer file sharing on the Internet. Any digital file could be shared, but, Internet traffic mostly consisted of hundred's of millions of US and European teenagers posting and sharing on their Internet connected, home personal computers illegal and unpaid for copies of MPEG 1 audio layer 3 (MP3), compressed, digital, music files which were made from NEVER encrypted Copyrighted music compact disks (CD's).

The Recording Industry Association of America (RIAA) estimated that Napster (R), and Gnutella (R) other similar types of services caused in year 2000 alone a loss of 2-3 several billion US dollars in yearly retail sales to the music industry out ^{approx} of ³² ~~50~~ billion in worldwide music sales and a loss of hundreds of millions of US dollars in yearly copyright royalties to the recording artists.

In the end of year 2000, Napster was declared in violation of the US Copyright laws by Federal district court judge Marilyn Hall Patel and forced into near bankruptcy by hefty fines, penalties, and settlements.

e.g. DIVXX (R) was an early commercial digital versatile disk (DVD) custom encryption format promoted by the Circuit City (R) electronics retail chain which needed a special cryptographic digital versatile disk (DVD) player. The encryption was custom or unique for each vendor, each player, and each customer. The format was tailored

for home rental movies rented on DVD format which was supposed to replace video cassette recorder (VCR) tape rental. The cryptographic procedure was similar to the Schenier portable music format explained in [REF 10]. DIVXX (R) failed in the marketplace because it was a proprietary non-standard format which failed to attract a de facto industry following.

e.g. In y. 2002, DIVX (R) with one less "X" has resurrected itself as an Internet distribution software format for MPEG IV compressed digital Internet distributed movies. The cryptographic medium even on fast cable modem and asymmetric digital subscriber lines (ADSL) phone modem lines takes a minimum of two hours to download a feature length commercial movie with analog color television quality. The standard is yet unknown but believed to be similar to its predecessor.

e.g. The content scrambling system (CSS) is an electronic system for scrambling audio/video digital versatile disk (DVD) content which was intended to keep mostly commercial movie digital versatile disk (DVD) content safe from hackers. Digital versatile disk (DVD) content was designed to be unlike the older compact disk (CD) content which was never encrypted and thus easily copied in digital master form.

In the late 1990's, the designers of Content Scrambling System (CSS) knowingly used weak hardware circuit encryption scrambling of movies when digital versatile disks (DVD's) first came out. The CSS

designers had a firm expectation that the encryption would be cracked by hackers within two to three years. Content scrambling system (CSS) used a known weak encryption hardware based duo-linear feedback shift register (duo-LFSR) technique with one LFSR dedicated to general family key encryption with a family initialization vector and one LFSR dedicated to custom movie distributor use with a unique vendor initialization vector. Each hardware DVD player would receive the family initialization vector (IV) stored in hardware and each distributed DVD would receive a software vendor initialization vector. The LFSR encryption was used to custom encrypt for each movie distribution company but standard for each customer and player the digital content on digital versatile disks (DVD) and decrypt the content in an authorized digital versatile disk (DVD) cryptographic media player [REF 508]. The vendor initialization vector was then family LFSR encrypted for "cipher text" storage on the DVD.

In 1999, the content scrambling system's (CSS) encryption was easily decrypted within months by a Swedish hacking group of teenagers called "Anathema" using personal computer (PC) based hacker "cracking programs." A single erring movie vendor had unintentionally left a "clear (decrypted) text" vendor initialization vector (IV) on his own distributed digital versatile disk's (DVD) which it sold. "Anathema" used the single unveiled vendor initialization vector (IV) to decrypt the other vendors' encrypted crypto keys. The family key initialization vector (IV) had already been cracked by inside authorized vendor sources leaking out computer program source code

information used for the Linux (R) brand of UNIX operating system production of DVD disks. Hackers had created a "De-CSS" computer program for Linux used to remove CSS scrambling which was available on hacker Web sites. "Anathema" released over two-thirds of the two thousand secret keys used by separate movie distribution companies to encrypt video digital masters along with the hacked out algorithm or cipher crypto-analysis "solution".

In the year 2000, the Recording Industry Association of America (RIAA) has launched the Secure Digital Music Initiative (SDMI) to establish open standards for secure, digital media distribution (see REFERENCES - Non-patent Related References [REF 500]).

RIAA has fielded request for proposals (RFP's) with the goal of developing industry wide open standards using the technologies of public key cryptography, secret key cryptography, and or analog and/or digital watermarks (a form of digital signatures which acts like a printed watermark on authorized paper documents) to uniquely identify authorized digital works, etc.

In y. 2001, a European academic published a crypto-analysis of the cryptography used in the Adobe (R) Corporation's electronic book (e-book) format to distribute over the World Wide Web (WWW) type-set text and photographs readable on a prior art Personal Computer (PC) using the Adobe (R) Acrobat Reader (R) with special Adobe (R) multi-master fonts (font imitations) which do not have to be down-loaded. The academic was charged in Federal Court by Adobe Corporation with violating the US Digital Millenium Act of y. 1998 which broadly

prohibited developing even the programming tools to attack or analyze ciphers used for US and Internationally Copyrighted commercial digital media distribution. A higher Federal Appeals Court put a suspension on the lower court ruling. At issue was not US Copyright violation, but, the 1st Amendment Freedom of Expression and INDEPENDENT FREE PRESS right of academic research into the cryptography tools used to implement the US Copyright violation restrictions. The US Digital Millenium Act of y. 1998 was ruled overly broad in effect trying to outlaw all language for one person's use of foul language. A Russian private corporation used the published cipher data obtained by its management in the US at a US hacker convention in Los Angeles and used the decryption algorithms to export to the US Copyright piracy software to illegally read Adobe electronic books in the US. A Federal court in y. 2002 ruled that the import into the US of the Russian piracy software could be blocked, but, the Russian corporation's employees were not in violation of the Digital Millenium Copyright Act of 1998 due to being Russian citizens unaware of US law and out of US jurisdiction.

In October of 2001, a proprietary, digital watermarking technique was selected as the first generation secure digital music initiative (SDMI) standard for digital music only intended for portable media players. Digital watermarking is not encryption, but, the use of unique and hidden digital markings to identify digital media much like an ink pattern watermark used upon letter paper. A hardcopy pen and paper analogy are the faint ink and sometimes embossed (raised letters and symbols) personal markings on letter-head corporate paper called hardcopy watermarks. In y. 2002, there is no technical or mathematical

evidence that even pseudo random (PR) digital watermarks cannot eventually be filtered out by hackers using powerful personal computer (PC) digital filter programs. This digital watermark if found on digital content is merely a Copyright identification, legal owner identification aid, music piece and version identification aid, and an aid in audit trail which identifies the legal copyright owner. The digital watermark also helps prevent illegal copying of the digitally watermarked digital media only if an authorized Secure Digital Music Initiative (SDMI) compliant portable media player is used. Customer playing of previous digital data such as Moving Picture Electronics Group (MPEG) standards I audio layer 3 (MP3) compressed digital music is not effected in any way even if illegally recorded and used (a SDMI industry courtesy to loyal fans and customers). Customer playing of non-watermarked and non-Copyrighted home produced material such as "home-brew" music is not effected in any way. The use of personal computers (PC's) are effected by the need of introducing new personal computer's (PC's) which would not copy digital music media having a Copyrighted watermark. This personal computer chore of monitoring for the Secure Digital Music Initiative (SDMI) music "digital watermark" for music would be in an addition to monitoring for the US National Association of Broadcasters (NAB) "broadcast flag" post-broadcast inserted only into "over the air" broadcast audio/video. The y. 2002 US Senate's Hollings Commerce Committee (which is in charge of Federal Communications Commission (FCC) controlling only the phone system, cable system, and US airways) has passed legislation which requires personal computer (PC) monitoring only of the "over the air" broadcast flag. The broadcast flag will be post-broadcast inserted by a digital

television set-top box into unencrypted "over the air" digital media in the new fully digital, standard definition television (SDTV) and high definition television (HDTV) broadcasts in order to prevent digital to digital copying of any form. Personal computers can digitally copy perfect limitless copies of digital media (e.g. DVD-RW, DVD+RW, CD-R, CD-RW, FLASH cards, or digital tape) to other digital media form. The SDMI Committee has also approved an imperceptible to music quality ("golden ear listeners"), analog audio watermark which will be added into analog audio output to loud-speakers to help identify wiretapped and digitally recorded analog audio output.

In August of 2002, the Secure Digital Music Initiative (SDMI) has not yet started a second generation more inclusive standards setting process yet. The second generation standard will use a more sophisticated cryptography technique than digital watermarks and analog watermarks, perhaps in the line of this invention involving customized per user hybrid key cryptography with media ticket smart cards.

The US Federal Communications Commission (FCC) and the US National Association of Broadcasters (NAB) are concerned about digital to digital recordings of all digital, high definition television (HDTV) "over-the-air" broadcasts for big screen TV's, and also digital standard definition television (SDTV) format with SDTV meant for backwards 483-viewable line compatibility with the existing analog TV's after digital to analog conversion (DAC) using a cheap "over the air" set-top box (about retail US \$300). A HDTV/SDTV "over the air" set-top box will receive all unencrypted, digital HDTV/SDTV television signals in MPEG II compressed digital form (compressed digital YCbCr form) and

convert them to two forms: 1). existing analog, National Television Standards Committee (NTSC) television signals for viewing upon existing NTSC analog television sets, 2). all digital HDTV/SDTV television signals can be displayed directly in digital form modulated to analog (analog Y'Cb'Cr') or in other words digital signals piggy-backed upon an analog carrier frequency for output upon the y. 2002 newly introduced, computer monitor like, high resolution, digital "big screen" television sets (which in y. 2002 cost about retail US \$1,500). All digital HDTV/SDTV signals are in y. 2002 broadcast "over the air" in unencrypted form. The "over the air" set-top boxes are vulnerable to 'digital to digital' signal theft unlike "over the air" analog NTSC signals and also unlike the 'cipher-text (encrypted)' cable TV set-top boxes and satellite TV set-top boxes which convert broadcast encrypted MPEG IV compressed digital audio/video for satellite set-top box conversion into unencrypted analog NTSC signals before wire-tappable output. "Over the air" set-top boxes using 'plain text (unencrypted text)' can allow unlimited and perfect 'digital to digital' copying of digital broadcast television shows and movies shown at home in either compressed digital MPEG X form or else in the much higher frequency uncompressed, digital modulated to analog (analog Y'Cb'Cr') form through signal sampling to reduce recording frequencies. The Digital Video Interface (DVI) of the Video Electronic Standards Association (VESA) was designed to counter 'digital to digital' 'set-top box' to digital monitor signal theft. All digital DVD-RW (R) recorders will allow perfect 'digital to digital copies' of these fully digital television shows for illegal copying and illegal distribution.

To prevent perfect digital copying upon digital recorders, the National Association of Broadcasters (NAB) wants the US Federal Communications Commission (FCC) to require a "broadcast flag" to be post-broadcast inserted by the antenna connected HDTV/SDTV "over the air" set-top box (not applying to the cable set-top box nor the satellite set-top box). The "broadcast flag" will be "over the air" set-top box post-reception inserted into the unencrypted "over the air" HDTV/SDTV signal. All electronics devices even personal computers capable of copying such digitally recorded "broadcast flag" marked digital media (e.g. DVD/RW (R) or DVD+RW (R) disks, CD-R (record once) disks, CD-RW (read/write) disks, FLASH memory disks, computer hard disks, streaming cassette tape) would then be required by law under the US Senate's Hollings Commerce Committee (in charge of Federal Communications (FCC) legislation) Bill of y. 2002 to detect the "broadcast flag" and stop illegal copying of US Copyrighted material. The Holling's Bill does not effect digital music using the Recording Industry Association of America's (RIAA's) Secure Digital Music Initiative (SDMI), Phase I digital watermark to identify Copyrighted music. The Holling's Bill also does not effect digital direct broadcast satellite (DBS) distribution services (e.g. Hughes Communication's DSS's (R), ~~New's Corporation/Echo Star's Dish Network~~ *Via com/ 22 12/24/2003* (R) signals) pre-encrypted audio/video, nor does it effect commercial theater satellite broadcasts which are pre-encrypted, nor does it effect cable broadcast standards similarly pre-encrypted. The US Senate's Leahy Judiciary Committee monitors the larger scope of US Copyright law in all forms besides just broadcast, cable, and phone line form.

The Electronics Industry Association (EIA) composed of commercial electronics and personal computer makers is sharply opposing the Hollings bill as a boondoggle for attorneys with a floodgate of future lawsuits, a pitifully weak technological defense against outside of US legal jurisdiction foreign pirates and hackers (who will not even have time to get a pizza before the weak electronic protections of weak digital watermarks on music and simple minded broadcast flags on "over the air" broadcasts are removed by automatic computer programs), and a major cost for consumer electronics manufacturers. The political reality agreed to by all parties is that the Hollings Committee Bill is a political scare tactic to get a better synergy of law/technology out of the technical community to stop Copyright piracy in its numerous electronic forms.

US digital direct broadcast satellite (DBS) service television signals (e.g. Hughes Communications (R) Direct Satellite Service (DSS (R), EchoStar (R)) is already sent in encrypted MPEG II compressed digital form for decryption by satellite set-top boxes with embedded in cryptographic memory family key (shared secret key) based hardware encryption (usually with no phone line connection [in older models without 'pay per view' special event programming] to the set-top box in the US unlike in Europe). This US satellite set-top box technology is unlike European satellite set-top boxes using satellite smart cards with phone line connections (see just below). The US satellite set-top box decrypts the signal and converts it into unencrypted, analog NTSC form for display upon color televisions. The analog NTSC satellite signal may be recorded upon prior art analog, video cassette recorder

(VCR) players. The satellite set-top box decryption of encrypted digital satellite signals for conversion to and output of compressed digital MPEG X SDTV/HDTV signals for input into full digital televisions (with a built-in set-top box) and also for separate output of uncompressed digital modulated to analog (very high frequency analog R'G'B') form for playing upon digital television monitors will also introduce chances of digital signal theft by digital to digital recording.

European all digital satellite channels are satellite transmitted in encrypted compressed digital form (compressed digital MPEG II which is not US HDTV/SDTV compatible) which is decrypted at the satellite set-top box for analog conversion to PAL, analog, audio/video TV signals (used in Great Britain and former British colonies) or SECAM, analog, audio/video TV signals (used in France or former French colonies). European satellite set-top box conversion plans for wire-tappable output of both HDTV/SDTV compressed digital signals for digital television (with a built-in set-top box) input and uncompressed digital output also known as digital modulated to analog (very high frequency analog R'G'B') output for display upon digital monitors is unknown. European satellite set-top boxes have a standard phone line (very unreliable) input and standard satellite smart card slots and readers with the satellite smart cards used as a cryptographic mini-database of special customer programming watched which are polled at least once a month by the satellite company computer over a phone modem and phone line for subsequent computer billing to credit cards or over the mail.

In y. 2002, US cable channels are transmitted over coaxial cable in broadband or with mixed analog and digital channels. Analog NTSC output channels are used for backwards compatibility with the existing 50 million US analog cable set-top boxes. [Encrypted] MPEG II compressed digital [modulated to analog for coaxial cable transmission (modulated or 'piggy-backed' digital) cable signals] are used with the new in y. 2002 US all digital cable set-top boxes. An all digital cable set-top box receives proprietary cable company format, unencrypted, compressed, fully digital, MPEG II signals (HDTV/SDTV MPEG X compatibility is not guaranteed) for decryption and analog conversion to NTSC signals for analog television display [(clearer and brighter analog components video (separated) NTSC color (HSI color model), as well as the much less clear and bright analog composite video (combined) NTSC color (HSI color model) is accepted as audio/video input by computer monitor like digital displays which must do a color model/matrix conversion to (gamma corrected) digital R'G'B' before display).] US cable all digital set-top box conversion plans to output both unencrypted HDTV/SDTV MPEG X compressed digital signals and/or digital modulated to analog (very high frequency analog R'G'B'). [computer monitor (S-video) output which gives the clearest and brightest picture of all, and/or unencrypted analog components video (HSCI color model separated NTSC signals), and/or the least clearest and least brightest unencrypted analog composite video (HSI color model combined color NTSC signals)] for display upon digital television [(with a built-in set-top box)] or digital computer monitors [(with an add-on set-top box of some form)] is unknown.

The US FCC has mandated a y. 2005 deadline for US transition of all "over the air" television stations to full digital "over the air" broadcast of unencrypted digital, high definition television (HDTV/SDTV) signal formats for digital television display and also conversion to analog NTSC format (for backwards compatibility with 80 million existing US analog televisions out of 60 million US households). US "over the air" set-top boxes will input unencrypted HDTV/SDTV (compressed digital MPEG X formats of many aspect ratios and progressive/interleaving formats) captured from "over the air" antennas and output unencrypted full digital modulated to analog (analog R'G'B') signals for digital monitor display and will separately output unencrypted HDTV/SDTV for digital television use (a digital monitor plus a built-in set-top box plus built-in digital tuner).

Any unencrypted digital signal and any such signal after digital to analog conversion (DAC) to its 1st generation analog signal output by a set-top box can be easily wiretapped and pirated with two alligator clips and an all digital audio/video recorder. A "real performance" stereo microphone fed digital tape recorder or hand-held digital videocamera at a movie premier screening can easily make "acceptable", low video quality, effectively non-stereo even with stereo (2-channel) microphones, digital masters of any actual "played" audio or video output. A pressing need exists for a common solution technology for the common and quite general problems of encrypted digital media distribution and a common any type of set-top box which will help prevent digital media piracy. This invention addresses many of these common problems.

Hughes Communication's (R) and Echostar's (R) Direct PC (R) provide direct satellite distribution service for the Internet which are popular and economic for rural area homes and businesses which due to sparse population induced economic infeasibilities, will never be serviced by fast broadband cable modem service (requires an existing cable system) and fast telephone line asymmetric digital subscriber line (ADSL) service (uses existing phone lines, but, phone lines must be of extremely high phone voice quality and also have a maximum range limitation of five miles from the phone company local office). The transmission control protocol/internet protocol (TCP/IP) internet protocol can use secret key encryption or public key encryption introduced at several TCP/IP protocol layers (e.g. secure sockets layer (SSL), secure transport layer, secure IP layer) and also can use as digital data digitally compressed MPEG X signals. The downstream from the satellite data link is 384 Kilo bits/second and the upstream back to the satellite data link is 56 Kilo bits/second.

The evolving field of Institute for Electronic and Electrical Engineers (IEEE) Standard IEEE 802.11a/b/c/g, "Wi-Fi" or "wireless high fidelity" land communications gives wireless radio frequency (RF) internet service in rural areas directly competing with direct broadcast satellite (DBS) distribution service at various data rates from 10 Mega bits/second up to 100 Mega bits/second and from ranges of 150 feet minimum out to a maximum range of up to twenty miles per home/business in rural areas. The "Wi-Fi" based internet service may be "skip stoned" from house to house and to business to house from a central rural town area which has direct fiber long distance phone

service from a long-distance telephone company local hub. The internet transmission control protocol internet protocol (TCP/IP) protocol signals are shared in a 'skip-stoned' configuration and must be custom encrypted for each home. The full-duplex (downstream and upstream) IEEE 802.11b data rate is 11 Mega bits/second with typical maximum range line of sight up to 15 to 20 miles. The much higher public access broadband frequency IEEE 802.11c gives 100 Mega/bits second of full-duplex wireless Ethernet access through non-metal walls up to 150 feet or 300 feet on a good day.

In the late 1990's, all digital commercial theater systems were announced using no movie film (e.g. Qualcomm's Commercial Theater, Boeing Commercial Theater Services using what was originally military satellite technology for secret key encrypting digital military data for satellite uplink and downlink). In addition, micro-mirror modules (MMM) took digital audio/video signals directly for direct projection theater systems. A red micro-mirror, green micro-mirror, and a blue micro-mirror (digital RGB) are required to alter projected beams of red, green, and blue light. In commercial digital theater systems, the movie distribution companies must turn their unencrypted digital masters over to a trusted 3rd party movie distribution corporation (e.g. Qualcomm (R), Boeing (R)). The 3rd party corporation will pre-uplink, secret key encrypt the digital streaming video for passage from a broadcast hub over leased fiber phone lines to a geo-stationary satellite uplink station, after which it is satellite broadcasted over dedicated geo-stationary satellite bandwidth, and satellite downlinked

to each local commercial movie theater. The downlink dish antenna produces an encrypted streaming video movie stream which is stored upon a theater held computer hard disk drive array in secret key encrypted form. At various repeating local theater showtimes, the encrypted digital video is personal computer read from the hard disk array, personal computer decrypted using projection hardware stored internal secret keys, personal computer accounting charged to the theater with ticket attendance data used for movie distribution company and artists' royalties, personal computer shown by a fully digital, Micro Mirror Module (MMM) projection system upon a wide movie screen with different screen sizes, the fully digital audio track with up to 30 audio channels of theater type sound (e.g. [Dolby Surround Sound (R) brand of theater sound system]) goes to a theater sound system for digital decompression (e.g. Dolby Theater Sound (R)) and digital to analog conversion (DAC) for the theater's 30 analog speakers, also digital multi-dimensional timing tracks are used for automatic theater lighting controls, intermissions and local advertising inserts.

The digital theater systems have been very slow to catch on. The \$100,000 to \$150,000 cost per digital projector must now be born by theater owners who are reluctant to capitalize this huge expense (they make their profits mostly off of the refreshments stand and break even on ticket sales after payment of labor costs, rents, and royalties to the movie distribution firms). The huge cost of \$10,000 per movie reel for digital master duplication to analog copies and secured distribution to individual theaters might be saved by the huge movie distribution companies, but, the huge movie distribution companies are

loathe to fully commit to digital master distribution which means that they must lose control of unencrypted digital masters (their "crown jewels") to a 3rd party corporation. Analog to analog copying is known to slowly produce degradation with every analog copy, so, analog copy distribution is not a matter of major concern to the movie distribution companies. Even with standard family key cryptography systems (shared secret keys by many parties) of secret key encryption, movie distribution companies fear that the family key will be obtained by hackers from an unattended digital movie projector leaving their "family crown jewels" in enemy hands.

This invention will try to overcome the shortcomings of the mentioned prior digital theater art in several fields. There is a pressing need for general solutions, for low cost solutions, for open standards, and for proprietary, new technology solutions in these fields which will benefit both governments and industry.

Prior Art Discussion of Cable Channel

Service Digital Media Distribution

Using Smart Cards

In y. 2002, US cable company (CABLECO) service set-top boxes also do not use inserted cable smart cards. Cable channels sent over broadband cable use of existing coaxial cable can have some pure analog channels (for backwards compatibility with 40 million existing US analog cable set-top boxes) and some pure digital channels (for use with emerging market US digital set-top boxes) as well as some channels dedicated to broadband cable digital internet use by home and business computers and also cable company digital billing services. The analog cable channels are broadcast in analog hardware circuit scrambled form which are analog hardware circuit de-scrambled at the older analog set-top box (for backwards compatibility with older analog set-top boxes). The digital cable channels are broadcast in digital family key encrypted form over MPEG IV compressed digital channels (for newer digital set-top boxes). The digital broadband cable internet service for home and business cable modems uses digital transmission control packet/internet protocol (TCP/IP) packet communications. All channel forms are supported by broadband cable service over coaxial cable. The family keys used for digital decryption are built into the newer cable set-top boxes using cryptographic memory. Older analog cable set-top

boxes used analog descrambling circuits which had secret circuit designs which were easily copied by cable pirate set-top box makers.

A US cable company "pay per bundle" monthly service charge was preferred by US cable companies with a base monthly charge and added premium service charges. "Pay per view" or special sports and live concert event viewing was implemented by US cable companies by requiring customers to pre-event and pre-broadcast phone call in to the cable company service center to get payment debited for viewing. The "cable loop" was then used at exact start of event or at start of broadcast by the cable company just like a local area network (LAN) connecting up to 30 US homes. The "cable loop" was used to specifically at exact start of event or start of broadcast to enable digital decryption on newer digital cable set-top boxes or else enable signal descrambling on older analog cable set-top boxes having analog hardware descrambling circuits.

In older analog cable set-top boxes, a special secret analog signal was sent from the cable company at the exact start of a "pay per view" show to start hardware descrambling circuits for the specific "pay per view" channel.

Prior Art Discussion of Direct Broadcast Service

(DBS) Digital Satellite

Service's Digital Media Distribution

Using Smart Cards

In y. 2002, prior art of specific digital media distribution weak and strong cryptography systems using portable and removable smart cards are few. The European satellite smart card inserted into satellite set-top box systems for controlling common encrypted satellite compressed digital signals are not used in the United States. The United States uses direct broadcast satellite (DBS) digital service set-top boxes such as older Direct Satellite Service (DSS (R)) from Hughes Communications (R) which prefers the technique of "pay per service bundle" with a base monthly charge plus added premium levels of service monthly charges. The Hughes Communications service does not satellite broadcast local channels which must be obtained by some other add-on product when in most rural areas cable television service is not and will never be available for economic reasons. The only other US commercial service is offered by ^{Echo Star RX 1/9/2004} News Corporation's Dish Network (R) which differentiates itself by offering a single roof-top satellite dish having two to four feed horns with two to four separate signals going to two to four separate 'set-top satellite boxes.' The newer Dish Network (R) satellites also use a spot broadcast beam which satellite broadcasts local television stations from the nearest metropolitan area. "Pay per service bundle" implementation does not require

satellite smart card set-top boxes. "Pay per service bundle" is implemented in the US with permanently embedding family keys (shared secret keys) within newer digital satellite set-top boxes using cryptographic memory or tamper resistant non-volatile memory (TNV-EEPROM) which family keys in turn are used for decrypting entire channel groups of common encrypted broadcast signals. Some US satellite set-top boxes require phone company input for 56 Kilo bits/second modem use for real-time 2-way communications with the central satellite company billing office which can remotely activate "pay per bundle" service or even individual "pay per view" events like live sports broadcasts and premier feature movies.

Older analog satellite set-top boxes used secret analog de-scrambling circuits which were often easily reverse engineered or made from stolen circuit diagrams.

Two main commercial systems are used for controlling home viewer access to European satellite television service with 30 million European viewers. The two main European suppliers are Canal Plus Technologies (R) with 12 million viewers and NDS (R) with most of the remainder. Canal Plus Technologies (R) is a division of French media conglomerate Vivendi Universal (R) once controlled by Mr. Jean Marie Messier with smart cards purchased by Vivendi (R) through an Italian subsidiary called Telepiu. Canal Plus' (R) main competitor was NDS (R) Corporation, a division of the huge News Corporation media conglomerate controlled by Australian financier Mr. Rupert Murdoch. A much smaller third satellite smart card supplier is Swiss based Kudelski Group (R). The main European entertainment fare media

protected by common encrypted transmissions of common MPEG X compressed digital video are "pay for view" soccer games, special music and stage concert events, and "XXX" pornographic movies.

The three main European satellite set-top box and smart card systems are non-compatible systems based upon different secret and proprietary standards which use pre-encrypted and pre-computer programmed smart cards. The European satellite set-top boxes have satellite smart card slots and media ticket smart card readers as well as a phone line connection. A predominant design consideration for European satellite set-top boxes is that the European phone line service is notoriously bad having 99% reliability or 1/100 calls failing for reasons other than busy phone lines or nobody home (no 99.999% AT&T reliability called 6 sigma reliability or less than 1/100,000 calls failing for technical reasons other than busy signals or no answer) with no central phone standards across European countries. In y. 2002, the extremely bad European phone service is a main reason why smart cards are highly popular in Europe for multiple uses, since, real-time phone line connections cannot be relied upon (inexpensive magnetic strip cards are dependent upon highly reliable real-time phone connections). European cable television service is in limited mountainous areas with satellite service preferred. The European satellite smart cards are customer inserted into satellite signal set-top boxes. The smart cards keep in cryptographic memory (tamper resistant non-volatile electrically erasable programmable read only memory (TNV-EEPROM)) both a secret computer billing program and a temporary secret mini-database record of what customer "pay for view"

shows are set-top box decrypted and watched. A periodic post-event, but, pre-monthly billing, central distribution entertainment company phone connection computer once a month inquiry to the phone-line connected set-top box can read the smart card's cryptographic mini-database. Given the un-reliable European phone lines and lack of phone standards, this billing phone inquiry can be tried multiple times with only one successful connection needed per month. The satellite distribution billing office can then post-event, properly bill each customer over the mail or over the internet.

In y. 2002, a US Federal District Court case filed by Canal Plus (R) under the US Copyright laws and the US Digital Millenium Copyright Act of y. 1998 alleges that the Canal Plus satellite smart card was infiltrated by a US 50 million dollar industrial and scientific espionage effort led by its rival NDS (R) through NDS Corporation's main scientific lab in Haifa, Israel. In y. 2002, the Canal Plus (R) satellite smart card's actual secret embedded source code had even been showing up on hacker Web sites. In y. 1999 (three years after market introduction), the Vivendi Universal (R) satellite systems had been plagued in Europe with up to a ratio of 3 to 1 illegal over legal Canal Plus (R) satellite smart cards used freely over paid legal satellite smart cards.

This form of satellite service smart card for a satellite set-top box is very different in purpose and implementation from the purposes of this invention.

SPECIFIC US PATENT PRIOR ART ON

PUBLIC KEY CRYPTOGRAPHY

MEDIA DISTRIBUTION SYSTEMS

Prior Art Patent Discussion On

Smart Cards

Many US Patent and Trademark Office (USPTO) and European Patent Office (EPO) patents have already been issued for smart cards, smart cash cards and distribution systems, smart phone cards, and smart voting cards. Smart cards have been extensively used in Europe for over fifteen years.

Smart cards have progressed rapidly in Europe in commercial and government uses despite their high relative cost (currently \$15.00 US dollars retail price) compared to magnetic strip cards (currently \$0.50 US dollars retail price) due to the poor reliability phone systems in Europe and the lack of central phone standards while the United States has always enjoyed reliable telecommunications and national phone standards. Magnetic strip cards require a reliable standardized phone system for real-time use.

In y. 2002, Monx (R) has many European Patent Office (EPO) patents on a system of forwards and backwards traceable cash passed by automatic teller machines to smart card to smart card to smart card back to automatic teller machine. DigiCash (R) has many patents for a non-compatible system of auditable cash transfer. Both electronic cash systems allow full tracing of transactions with a single point failure or in other words if any one smart card in a transfer chain is completely lost. The mathematics of this strong cryptography and secure hardware is very complicated and error prone.

In y. 2002, Sun Microsystems (R) has patents on Java (R) virtual machine (VM) architectures for smart cards. In y. 2002, these smart card systems are used for electronic cash and credit card systems by the US Army which is aiming for a "paperless office." Some systems also provide "card key" or access smart card types of security systems for US Army bases and US Navy aircraft carriers. The Java (R) smart security card can internally store a digital fingerprint model for comparison with the user's index finger inserted into a smart card reader attached to a personal computer.

"Java Smart Cards" are slow due to the firmware interpreted virtual machine (VM) architecture. In y. 2002, the Java Smart Cards have been found to be bug prone giving hacker access to many "secure" card key access systems.

In y. 2002, American Express has issued its "Blue" smart credit card. This "Blue" card can internally store small amounts of electronic cash and otherwise functions as a more secure form of credit card than the older magnetic strip credit cards. A photo-identification is printed on the front along with a visible light laser holograph. Internal storage of a digital fingerprint is done, but, currently is not widely used yet in the US due to a lack of fingerprint reader stations.

Registered US Patent No. 6,367,019

Issued to Ansell, Steven T., et. al.,

et. Schneier, Bruce

Assigned to: Liquid Audio Inc.

Issue Date: XX/XX/XX

Filing Date: XX/XX/XX

US Patent No. 6,367,019 [REF 10] also called the "Schneier portable music format patent" is a method of using a session key (one-time secret key) taken from the digital music which is used to custom, encrypt the distributed digital music and then the session key in turn is encrypted with a unique per owner family key (common pre-registered secret key only known by the media distribution company and also authorized hardware for one owner) for internet distribution of the encrypted session key downloaded along with the encrypted media. The custom, encrypted media with encrypted session key can thus be played only in an authorized media music player which has a unique per owner family key to decrypt the session key which in turn is used to decrypt the custom, encrypted digital media. The unique per owner family key can be common among the owner's several authorized digital media

players assuming some method of pre-installing or else customer portability and injection of the common key from and to his common media players (such a method is specified). The unique per owner family key is the same key exposed to all digital media distribution vendors, since the session key (1-time secret key) used to encrypt the digital media must be distribution vendor encrypted with the family key before being placed into the down-load digital media. Digital media distribution vendors are all fully trusted members of the system with access to all 'crown jewel' 'plain text (decrypted)' digital masters of every participating vendor, and have access to all customer family keys in a shared secret database.

The encrypted session key (one-time use secret key) varies for each customer and furthermore varies for each customer's music piece. A message authentication cipher (MAC) which is a message digest cipher (MDC) with a secret initialization vector (IV) can be computed for the digital media to produce an output fixed bit (e.g. 256-bit) MAC code. The MAC code can be session key encrypted to form a data integrity (wholeness or non-tampering) check also called a secret key digital signature. The session key encrypted MAC code can be optionally included as an integrity check in the downloaded custom encrypted digital media along with the unique per owner family key encrypted session key. Prior art serial data buses are mentioned as a non-secure way to transport cryptographic keys from a personal computer used for internet download to one authorized portable media player to another. Smart cards are mentioned in the patent as a cryptographically secure vessel for customers to transport the unique per owner family key and

unencrypted session key around in for injection into all of a customer's authorized media players.

The Schneier portable music patent is defective under the inventor's cryptanalysis in several regards which will render multi-million dollar music digital masters available to hackers within two months of release.

1). The unique per owner family key encrypted session key is not serial numbered or time stamped for customer portability and injection into other media players rendering the key definitely breachable by a known hacker attack called a "recorded replay attack" in which the hacker does not even need to family decrypt the session key. The hacker merely records the whole unique per owner family key encrypted session key or removes it from the download media. The whole recorded unique per owner family key encrypted session key is hacker distributed along with the recorded session key encrypted media and replayed on the common unique per owner family key media players. Whichever media players have a unique per owner family key (common secret key) can thus use the "recorded replay attack" recorded unique per owner family key encrypted session key without ever needing to unique per owner family key decrypt the session key. The unique per owner family key held in prior art electrically erasable programmable read only memory (EEPROM) is vulnerable to any hacker using a pin-prober or else an in-circuit emulator (ICE). What is required is the use of tamper resistant non-volatile electrically erasable programmable read only memory (TNV-EEPROM) which detects pin probers by

impedance loading and automatically erases its cryptographic memory.

2). The use of prior art serial data buses to transport non-pass-thru encrypted cryptographic keys is vulnerable to wiretapping which makes the cryptographic keys totally exposed to any hacker attacks thus revealing multi-million dollar digital masters.

3). The use of smart cards to receive non-pass-thru encrypted cryptographic keys which are also not public key encrypted or secret key encrypted to make them unique for a single customer or vendor means that any hacker can insert his own smart card and use and even read the deposited unencrypted cryptographic keys.

4). The use of only one unique per owner family key (common secret key) restricted to all authorized vendors of music and all authorized vendors of media players means that all vendors must trust each other. A cheating vendor can leak out multi-million dollar digital masters owned by another vendor. One vendor losing or having the single system unique per owner family key lost or stolen will compromise the entire system including every vendor's multi-million dollar digital masters. This type of attack has already occurred with the hacker group "Anathema's" attack upon the known weak hardware based duo-linear feed-back shift register (duo-LFSR) system used in the Content Scrambling System (CSS) for digital versatile disks (DVD's).

5). The use of non-cryptographic micro-processors (u-P's) and non-cryptographic digital signal processor's (DSP's) inside of

the portable music player to decrypt the custom encrypted digital music with the session key (1-time secret key) means that a skilled chip hacker using pin-probers, in-circuit emulators (ICE), or logic state analyzers will easily pick out the unencrypted cryptographic keys for his own use and distribution.

6). The absense of play counts to control the paid for number of plays, -1 for indefinite plays, or counts of free trial plays. Any Schneier authorized media player with a unique per owner family key and appropriate session key can play the media an infinite number of times. The Schneier authorized media player also has no method to restrict its infinite plays to a fixed number of plays as in 10 free trial music plays.

7). The "fair use" or legal US Copyright protected right of homeowners to make one or two copies of US Copyrighted media for their own use and legal archiving is not supported. Even having a single copy of encrypted media work both at a home CD-R player and in a car CD player is not permitted which is "fair use." The encrypted media can be owner copied an unlimited number of times. However, the matching unique per owner family key encrypted session key is kept in a Schneier portable media player's memory. If the Schneier portable media player is lost, stolen, or of disputed ownership, thousands of dollars worth of custom encrypted media recordings will be unplayable. If the matching unique per owner family key encrypted session key is kept in a single media ticket smart card for portability and injection into a portable media

player's memory, no method is specified for handling defective, lost, stolen, or disputed legal ownership media ticket smart cards.

8). The "first use" or legal US Copyright protected right of homeowners to sell or completely transfer legally owned US Copyrighted media to another person is not supported. The encrypted media can be owner copied an unlimited number of times. However, the matching unique per owner family key encrypted session key is kept in a Schneier portable media player's memory. The Schneier portable media player with all of its matching custom digital media can be sold or given away in entirety as a matched set. If the matching unique per owner family key encrypted session key is kept in a single, media ticket smart card for portability with injection into the portable media player's memory, the media ticket smart card can be sold along with the custom encrypted physical media. No method is specified for handling defective, lost, stolen, or disputed legal ownership media ticket smart cards.

The inventor's patent avoids all of these hacker attack points by offering a cryptographically sound digital media distribution system using strong cryptography and all cryptographic hardware based key containment. The inventor's patent uses serial numbers to stop recorded replay attacks which is a known technique where a digital clock is not universally available for the alternate time stamp technique. The inventor's patent restricts cryptographic keys to

cryptographic memory and cryptographic hardware with pass-thru encryption used across all wiretappable or "red" computer buses.

The inventor's patent supports "play codes" which are session key or 1-time secret keys and "play counts" which are paid for numbers of plays, -1 for infinite plays, or counts of free trial plays which furthermore are:

1stly, vendor digitally signed (with a unique vendor private key) with an added sequence number,

2ndly, unique vendor secret key encrypted, and

3rdly, uniquely customer private key encrypted, and

4thly, media ticket smart card system family key encrypted in order to restrict play counts to one vendor and one customer which allows accounting functions for the media.

Registered US Patent No. 5,315,658

Issued to: Micali, Silvio

Issue Date:

Filing Date:

Registered US Patent No. 5,315,658 [REF 300] develops a "fair and fail-safe key escrow" system after a "subliminal channel" was found in his previous "fair key escrow" of US Patent No. 5,276,737. A subliminal channel was found in his key splitting and key escrow technique for Diffie-Hellman (R) in his first Diffie-Hellman (R) "fair escrow" patent. A "subliminal channel" allows a user to send a totally concealed and undetectable message (which might even be the full private key) to the key escrow parties or the public key distribution authority. The "fail-safe key escrow" system eliminates this subliminal channel.

My patent optionally uses key escrow of which a specific use can be Micali key escrow for escrowing cryptographic keys for the purposes of customer lost or stolen keys, customer disputes over legal key ownership, and court orders to retrieve split keys for use by law enforcement.

Registered US Patent No. 5,276,737

Issued to: Micali, Silvio

Issue Date:

Filing Date:

Registered US Patent No. 5,276,737 [REF 304] has been issued to Silvio Micali for a specific public key cryptography based system of key escrow using split keys in a system known as "fair key escrow". Now transferred to Banker's Trust of New York with a license purchased by the National Institute of Standards and Technology's (NIST's) Clipper and Capstone cryptography projects. The "fair crypto-systems" allow Diffie-Hellman (R) [REF 6] and RSA (R) [REF 5] algorithm users to do private key splitting of keys into key pieces and private key piece escrow with various key escrow parties under supervision of a public key distribution authority in a specific mathematical manner with nice legal objectives. This specific technique using allows the key distribution authority to verify the split key pieces held by the various key escrow parties without disclosing of the full private key to any one party, which is quite a neat trick. The Diffie-Hellman (R) fair escrow technique uses discrete logarithms computed on split key pieces. The RSA (R) fair escrow technique uses Blum integers. The split keys in an RSA (R) fair escrow technique is also combined with a flexible, majority voting scheme which requires any three out of five escrow parties to combine private key pieces before a full private key is formed.

This proposed patent optionally uses key escrow of which a specific use can be Micali key escrow for escrowing cryptographic keys for the purposes of customer lost or stolen keys, customer disputes over legal key ownership settled by court order, and court orders to retrieve split keys for use by law enforcement.

Registered US Patent No. 5,231,668

Issued to: Kravitz, David

Issue Date:

Filing Date:

A Registered US Patent Number No. 5,231,668 [REF 308] has been issued to David Kravitz formerly of the US National Security Agency for the digital signature algorithm (DSA). This patent does only digital signatures and not encryption, decryption, or cryptographic key exchanges.

Registered US Patent No. 4,405,829

Issued to: Rivest, Shamir, and Adleman (RSA)

Issue Date:

Filing Date:

A Registered US Patent Number No. 4,405,829 [REF 316] has been issued to Rivest, Shamir, and Adleman (RSA), now transferred to Public Key Partners (R), for the RSA public key cryptology algorithm. A public key cryptography environment and different architectures based upon RSA is protected by this patent. This patent expired in y. 1999 and RSA (R) is now in the public domain.

Registered US Patent No. 4,200,770

Issued to: Diffie, Winn &

Hellman, Martin

Issue Date:

Filing Date:

A Registered US Patent Number No. 4,200,770 (Diffie, Hellman public key exchange algorithm) [REF 320] has been issued on TBD for the first proven public key cryptography key exchange algorithm.

SUMMARY

A new process or methods of systems invention of cryptographic architecture for electronic distribution of custom encrypted digital media over the internet for deposit upon physical media or for direct physical, commercial physical distribution of custom encrypted digital media which uses internet updatable media ticket smart cards holding play codes (session keys or 1-time secret keys) and play codes (paid for numbers of plays, -1 for indefinite plays, or counts of free trial plays) which physically distributed "footprint downloaded" digital media and media ticket smart card is inserted into a cryptographic media player with a built-in media ticket smart card reader for playing.

A 1st alternative embodiment invention of a custom encrypted high definition television (HDTV) or standard definition digital television (SDTV) signal transmitted "over the airwaves", or else transmitted over fast digital broadband cable modem lines, or else transmitted over fast digital broadband asymmetric digital subscriber phone lines (ADSL), or else transmitted over direct satellite service (DSS) systems or else transmitted over "wireless Ethernet" "stone skipped" systems to homes or businesses with a cryptographic media player set-top box with a built-in media ticket smart card reader with a properly matched media ticket smart card which in turn is connected to a digital television/digital audio/digital video recorder. The HDTV/SDTV signal may have embedded MPEG II extensions for very efficient background data or cryptography "silhouette-like" technique electronic television guide

information using a spreadsheet or matrix type of graphical user interface (GUI) which will give a digital picture in the picture (PIP) electronic television guide display and means of future program recording.

A 2nd alternative embodiment invention of a rack of digital versatile disk (DVD) drives holding digital versatile disks which are vendor pre-programmed and physically distributed custom encrypted digital medium played upon a movie cryptographic media player/digital versatile disk drive/micro-mirror machine module (MMM)/theater projection and sound system with a built-in media ticket smart card reader with an inserted proper media ticket smart card.

OBJECTS & ADVANTAGES - vs. PRIOR ART

A. An object of this invention is to support physical and electronic internet "downloaded" distribution of custom encrypted digital media limited to digital music, digital movies, digital newspapers, and digital books (not including digital computer programs, digital computer games, and digital computer multi-media) (see REFERENCES - NON-PATENT LITERATURE [REF 500] - "The Secure Digital Music Initiative (SDMI)") for "playing" or decryption of the portable media upon special cryptographic media players.

Napster (R) and Gnutella (R) types of peer to peer web music distribution services of movie picture electronics group (MPEG 1 audio layer 3 also called MP3) compressed digital music files allow customers to widely distribute illegal, copyright protected media. The MP3 files are customer created at home personal computers reading non-encrypted music compact disk sources. The music digital master on the compact disks are totally unprotected from illegal copyright piracy.

B. An object of this invention is to use only one media ticket smart card per owner of the corresponding digital media from many different media distribution vendors of digital music, digital movies, electronic newspapers, and electronic books.

One media ticket smart card per music company or one media ticket smart card per item of music will be burdensome and confusing to the customer.

Prior art floppy based or dongle based or keychain based cryptographic key storage was matched one to one with a piece of encrypted data.

C. An object of this invention is to allow the owner's one media ticket smart card to be used with any owner's cryptographic media player [REF 508].

Having one media ticket smart card matched to only the owner's single cryptographic media player [REF 508] will be confusing and limit the choice of players.

D. An object of this invention is to stop the use of any unauthorized digital copying of digital media.

Napster (R) types of peer to peer web music distribution services of movie picture electronics group compressed digital music files (MP3) which allow customers to widely distribute illegal, copyright protected media. The MP3 files are customer created at home personal computers (PC's) reading non-encrypted music compact disk (CD) sources. The music digital master on the compact disks are totally unprotected from illegal copyright piracy.

Taiwanese music piracy operations routinely legally copy music cassette tapes, music compact disks, and movie video cassette tapes for overseas distribution into countries not in the international copyright convention. The unencrypted music and movie analog and digital masters are vulnerable and not technologically protected.

E. An object of this invention is to restrict one digital media distribution company's unencrypted digital masters only to itself and absolutely no other party especially prohibiting access by any other competing digital media distribution company.

F. An object of this invention is to allow play counts or count controlled plays or counted decryptions of custom encrypted media including counts of free trial media plays.

Unencrypted digital media can be used an unlimited number of times and allow unlimited perfect copying of digital masters for distribution to unlimited numbers of people.

G. An object of this invention is to provide all public key cryptography legal attributes such as:

- 1). authentication (like an exchange of photo ID's or thumbprints)

- 2). encryption/decryption (for privacy)

- 3). integrity (wholeness or non-tampering)
- 4). digital signatures (like handwritten signatures)
- 5). non-repudiation (denying digital signatures)
- 6). authorization (approval using digital signatures and dating or official post marks)
- 7). archiving (storing digitally signed documents in a high integrity environment)
- 8). accessibility (restricting access to authorized users)
- 9). audit trail (recording accesses to information with public key ID's, dates, times, and locations)
- 10). play counts/play codes for counting paid for and authorized personally encrypted digital media plays and for decrypting them
- 11). crypto key splitting and key escrow.
- 12). crypto key administration and key architectures. Digital media without encryption cannot implement these legal attributes.

H. An object of this invention is to support pass-thru encryption of cryptographic keys called play codes (session keys or 1-time secret keys) and play counts (paid for numbers of plays, -1 for indefinite plays, or counts of free trial plays) for their trip from a media distribution company's central web server over the open internet to a customer's personal computer over wiretappable buses to a secure,

cryptographic memory inside of a smart card which is inserted into a media ticket smart card reader attached to the same personal computer.

Prior art cryptographic systems have relied upon secure sockets layer (SSL) types of public key distribution. Secure sockets layer does not store cryptographic keys in cryptographic memory. It also does not use pass-thru encryption over wiretappable computer buses. Secure sockets layer is vulnerable to hacker cryptographic algorithm disassembly attacks, logic analyzer attacks, hard disk copying and automated password decryption on hard disk hacker programs, keyboard capture buffers, etc.

I. An object of this invention is to support physical transfer of encrypted digital media in the form of digital versatile disk read/write (DVD-RW (R), DVD+RW (R)), compact disk record once (CD-R (R)), and bank programmable solid state memory cards (FLASH (R)) and also the physical transfer of media ticket smart cards from a customer's personal computer (PC) to a cryptographic media player [REF 508] (e.g. crypto-MP3) into which both are inserted.

J. An object of this invention is to support pass-thru encryption of cryptographic keys in the form of play codes (session keys or 1-time secret keys) and play counts (paid for numbers of plays, -1 for indefinite plays, or counts of free trial plays) from a media ticket smart card inserted into a media ticket smart card reader built-into a cryptographic media player [REF 508] for transferring such keys over wiretappable ("red") computer buses to a cryptographic digital signal processor unit [REF 500], having its own tamper resistant non-volatile

electrically erasable programmable read only memory which processor is contained inside of the cryptographic media player [REF 508].

Examples are pass-thru, encrypted, transfer of keys from smart cards to media ticket smart card readers (using media ticket smart card reader vendor family keys) to cryptographic-DSP's (using cryptographic-DSP vendor family keys).

K. An object of this invention is to support an optional citizen/customer media ticket smart card authentication triangle between the three points of:

point 1, customer A to (identified by a 1st means of a passphrase/passcode, a 2nd means of a bio-identification such as a digital fingerprint, a 3rd means of a password with pseudorandom noise mixed in), to

point 2, media ticket smart card A holding a customer, or user's private keys, secret keys, password with pseudorandom noise mixed in, bio-identification such as a digital fingerprint, session keys, play codes, and play counts to prevent the use of stolen media ticket smart cards, to

point 3, cryptographic media player [REF 508].

Any one of the three points which are detected as unauthorized will stop the media ticket smart card read/write process.

L. An object of this invention is to support a cryptographic media authentication triangle between the three points of:

point 1, a copy of 1-way transferred and custom session key encrypted digital media, to

point 2, media ticket smart card holding a customer, or user's private keys, secret keys, session keys, play codes, and play counts, to

point 3, cryptographic media player [REF 508].

Any one of the three points which are detected as unauthorized will stop the custom encrypted digital media playing process.

M. An object of this invention is to support legal "fair use" of US copyrighted encrypted digital media or the archiving of two to three copies for personal use. The purpose of "fair use" is to allow for recovery in case of accidental damage, theft, fire, flood, natural disaster, legal archiving, disputed legal ownership (as any divorced person will recognise), or one or at most two convenience copies in multiple locations used by the legal owner. Legal "fair use" also supports a home set of media and an auto set of media.

N. An object of this invention is to support legal "first use" of US copyrighted encrypted digital media or the right of one person to sell or transfer in entirety the encrypted digital media to another person and transfer only relevant media ticket smart card cryptographic keys to the other person's media ticket smart card.

O. An object of this invention is to support lost and stolen media ticket smart cards.

P. An object of this invention is to support non-copyrighted commercial material, home produced material, and previously recorded, prior art, non-encrypted digital Copyrighted material by allowing unlimited unencrypted plays of the media.

Q. An object of this invention is to prevent use of this strong cryptography system of software and hardware by terrorist forces and countries which are enemies of the United States for military use of Command, Control, Communications, Computers, and Coordination (CCCCC or C Five).

=====

R. In the 1st alternative embodiment, an object of this invention is to support custom encrypted MPEG X audio layer 3 (MP3) compressed digital audio, custom encrypted digital standard broadcast (SDTV), and digital high definition "bigscreen" television (HDTV) in digital "over the air" transmitted signals, or else cable distributed digital signals using high speed broadband cable modems, or else phone line distributed signals using high speed asymmetric digital subscriber line (ADSL) broadband modems, or else direct broadcast satellite (DBS) service transmitted signals, or "wireless Ethernet" Institute for Electrical and Electronic Engineers Standard 802.11c (100 Mega bits/second) transmitted "skip stoned" signals, which are all custom decrypted using a cryptographic set-top box with a built-in media ticket smart card reader with an inserted matching media ticket smart card which is further attached to a digital television monitor. A digital television merely has a built-in set-top box of some form. The set-top box may have an additional attached audio/video digital recorder of some form or some level of intelligence.

The HDTV/SDTV signal may have a non-standard MPEG II extension for a very efficient cryptography "silhouette-like" technique background scene cutting and replacement method of introducing electronic television guide digital data. The digital picture in a picture will present the electronic television guide data in a spreadsheet style or matrix style of graphical user interface (GUI) for current program selection and future program recording.

S. In the 2nd alternative embodiment, an object of this invention is to support a high performance, movie cryptographic media player/micro-mirror machine module (MMM) for commercial movie theater use.

Z. Further objects and advantages of my invention will become apparent from a consideration of the drawings and ensuing description of it.

BRIEF DESCRIPTION OF DRAWINGS - All Embodiments

Fig. 1 is a pyramid showing the layered design of the full proposed cryptographic system and where the media ticket smart card and media ticket smart card custom encrypted digital media distribution public key cryptography architecture is suggested as an embodiment.

Fig. 2 is a circuit block diagram of a prior art cryptographic microprocessor unit found in a prior art smart card.

Fig. 3 is a circuit block diagram of a prior art media ticket smart card (212). This is used for secret key and private key secure containment and physical transportation.

Fig. 4 is a circuit block diagram of a prior art media ticket smart card reader attached to a personal computer.

Fig. 5 is a circuit block diagram of a cryptographic digital signal processor (C-DSP) (932) future patent pending [REF 500]. This is used for doing hybrid key cryptography which is both public key cryptography and fast hardware based secret key cryptography inside of a digital signal processor processing digital signals in a cryptographically secure environment.

Fig. 6 is a circuit block diagram of a cryptographic media player, future patent pending [REF 508] with a built-in media ticket smart card reader.

Fig. 7 is a unit block diagram of the 1st alternative embodiment of a universal input cryptographic set-top box for encrypted or "cipher text" high definition television (HDTV)/standard definition television (SDTV) signals coming "over the airwaves", by cable system, by phone system, by satellite, or by IEEE 802.11c wireless Ethernet connections.

Fig. 8 is a circuit block diagram of the 1st alternative embodiment of a universal input cryptographic set-top box for encrypted or "cipher text" high definition television (HDTV)/standard definition television (SDTV) signals coming "over the airwaves", by cable system, by phone system, by satellite, or by IEEE 802.11c wireless Ethernet connections.

Fig. 9 is a circuit block diagram of the 2nd alternative embodiment of a cryptographic micro mirror module (MMM) commercial movie theater system.

LIST OF REFERENCE NUMERALS - All Embodiments

100. media ticket smart card custom encrypted digital media public key cryptography federated architecture.

104. media ticket smart card system authority (party S):

108. central public key generation authority (C-PuKGA) (party G),

112. central public key distribution authority (C-PuKDA) (party D),

NOTE: also called a central public key certificate
authority (C-CA),

116. central public key distribution authority database ID number
N (media ticket smart card system authority controlled or
administered) (C-PuKDA-N),

N = 0 is reserved for the US government,

N > 1 is used by a foreign government,

120. central public key distribution authority key escrow agent A
(C-PuKEA-A) (party E1),

124. central public key distribution authority key escrow agent B
(C-PuKEA-B) (party E2).

128. digital media distribution vendors (party V).

160. 1-way transfer and custom session key encrypted copyrighted digital media in data form (movies, videos, music, newspapers, books) which may be digitally compressed MPEG IV audio/video files or digitally compressed MPEG I audio layer 3 (MP3) music files.

PARTS OF 1ST ALTERNATIVE EMBODIMENT ONLY:

700. universal "over the air," cable line, phone line ADSL, satellite, and Institute of Electrical and Electronic Engineers (IEEE) 802.11c HDTV/SDTV signal set-top boxes (1st alternative embodiment) with embedded crypto digital signal processing (C-DSP) units (932):

704. radio frequency (RF) antenna input (broadcast airwaves),

705. micro-wave radio frequency (RF) direct satellite dish input,

706. IEEE 802.11c wireless Ethernet "Wi-Fi" "skip-stoned" input,

707a. modulated digital coaxial cable input (cable companies (CABLECO'S)),

707b. modulated digital fast asymmetric digital subscriber line (ADSL) modem, twisted pair, copper, phone line input (telephone companies (TELCO'S)),

708a. radio frequency (RF) to intermediate frequency
(IF) down-conversion circuitry,

708b. analog to digital circuitry (ADC),

708c. digital tuner,

708d. video RAM for "picture in a picture (PIP)"
digital display of the electronic television guide data
(extracted by added circuitry to the secret key decryption
circuitry from the new cryptography "silhouette-like" technique,
non-MPEG X standard, extension to the MPEG I, II, or MPEG IV
standard audio/video signals),

708e. audio output digital to analog converters (DAC's),

708f. line amplifiers,

708g. 5.1-channel theater analog audio system
output of 5 units of tweeter, mid-range, and woofer and 1 unit
of stand alone deep-bass woofer unit,

709a. video output RAM digital to analog converters
(RAMDAC's),

709b. line amplifiers,

709c. HDTV/SDTV video output which is artificially

digitally degraded by the MPEG X de-compression circuitry
and converted to modulated digital UXGA computer formats
for computer monitors and digital television monitors,

709d. "cipher text" compressed digital MPEG IV audio/video

digital output for digital recording in DVD-RW (R), or DVD+RW R)
drives with media,

709e. enhancement option) "cipher text" compressed

digital MPEG IV audio/video digital output for digital recording
on bank programmable memory cards (FLASH EEPROM),

709f. matrix transform circuits for digital MPEG X yellow

(Y), cobalt blue (Cb), chromium red (Cr) color model (YCbCr)
signal conversion to various analog composite video signal
formats such as NTSC (US , Japan, and US colonies), PAL (United
Kingdom and UK colonies), or SECAM (France and French colonies),

709g. radio frequency (RF) modulated artificially

digitally degraded analog output for injection into prior art
analog NTSC, PAL, SECAM televisions,

709h. s-video or analog non-composite video output and

conversion circuitry,

711. infrared remote (IR) control unit

712. infrared remote (IR) control circuitry

715. has a built-in media ticket smart card reader,

716. has a built-in toggle field with liquid crystal display (LCD) and controls for up to 10 alpha-numeric characters for passphrase/passcode entry,

717. (future option) has a built-in bio-identification unit and interface circuitry such as a digitized fingerprint reader,

718. (convenience option) has a built-in digital recorder and interface circuitry such as a digital versatile disk read/write (DVD-RW (R) or DVD+RW (R)) drive,

719. (convenience option) with a broadband cable modem or broadband ADSL Internet connection can have an upgraded cryptographic digital signal processor to a cryptographic strong advanced risk micro-processor (strong-ARM) for a Web television type of set-top box with a keyboard input port.

PARTS OF 2ND ALTERNATIVE EMBODIMENT ONLY:

720. external micro-mirror module (MMM) movie theater players (2nd alternative embodiment) with embedded crypto digital signal processing units (932):

721. micro-mirror module (MMM) with three digital micro-mirrors for red, green, and blue projection lamps,

722. digital versatile disk (DVD) movie set input, (four or more double sided, double density DVD disks or at least two disks per intermission),

724. theater projector light output (red, green, blue) from three micro-mirror module (MMM) units and three color projection lamps,

726. 30-channel theater sound analog audio system output n-dimensional theater experience digital output,

727. 30 units of speakers for movie theater theater-type sound,

730. has a built-in media ticket smart card reader,

732. has a built-in toggle field with liquid crystal display (LCD) and controls for up to 10 alpha-numeric characters for passphrase/passcode entry,

734. (future option) has a built-in bio-identification unit such as a fingerprint reader,

740. digital timing and control outputs for multi-dimensional sensory units such as seat vibration units, olfactory (smell) units, special effect colored laser lights and displays, special effect explosions, automatic theater drapery and light timing controls,

744. seat vibration unit digital control line,

748. seat olfactory unit digital control line

(e.g. perfume, gunpowder, cologne, cigar smoke, flowers, dust, etc.),

752. society of motion picture and theater entertainment (SMPTE) sound and light, automatic theater drapery, serial data command and response control and high rate digital serial timing line,

756. automatic drapery timing unit needing digital clock synchronization to the start of the movie,

760. automatic theater light timing unit needing

digital clock synchronization to the start of the movie.

NOT PART OF INVENTION:

800. internet.

802. customers.

804. internet protocol (IP) packet.

808. world wide web (WWW) graphics intense portion of the internet.

812. digital versatile disks (DVD's) (DVD, DVD-RW (R), DVD+RW (R)).

816. compact disks (CD's) (CD, CD-R (R), CD-RW (R)).

820. personal computer's (PC's).

Prior art units equipped with an internet connection, world wide web (WWW) browser, and media ticket smart card reader, and prior art drives such as compact disk record once (CD-R), digital versatile disk read/write (DVD-RW (R), DVD+RW (R)), flash solid state memory.

824. web server computers media distribution company office web server computers which distribute custom encrypted digital media

downloaded by the internet to customer's personal computers. These server computers must be physically contained in US National Computer Security Center (NCSC) classified commercial rated C2 facilities (physically isolated and locked with Internet connections) with layered security highly protected inner-sanctum for 'plain-text (unencrypted)' digital master storage and conversion to custom 'cipher-text (encrypted)' media, layered security, and final Internet layer firewall protection.

840. crypto micro-processor/micro-controller (C-uP's):

844. embedded micro-controller (single chip micro-processor with built-in bus interface (I/O), timing circuitry or counter timer circuitry(CTC), DRAM refresh and addressing circuitry, direct memory access or DMA circuitry,

848. intermetallic layer wire mesh with impedance monitoring for use as an anti-tamper device which will erase the cryptographic memory,

852. micro-controller bus,

856. a small amount of DRAM (temporary data store), or static RAM (SRAM),

860. a small amount of EEPROM (permanent program store),

864. cryptographic memory or tamper resistant non-volatile

electrically erasable programmable read only memory (TNV-EEPROM)
for permanent cryptographic program store and cryptographic data
store.

880. (media ticket) smart cards:

crypto-micro-controller (820),

884. calculator battery,

888. male card edge metallic contact with power pin

(for re-charging the battery).

900. (media ticket) smart card readers:

904. universal serial bus interface (to a personal
computer),

908. female card edge contact reader,

possibly cryptographic micro-processor for pass-thru encryption

(not needed if data is already family key encrypted) (820).

920. high security operating systems (HS-OS's). These are
high-security, operating systems which execute upon non-crypto-
CPU's. These must be physically contained in US National
Computer Security Center (NCSC) classified high security

(COMSEC) rated C3 or commercial restricted access facilities.

World wide web server computers with firewall protection.

924. local area networks (LAN's).

928. wide area networks (WAN's).

932. cryptographic digital signal processors (C-DSP's)
patent pending [REF 500], consisting of a single chip solution of
combined analog and digital silicon library (silicon compiler)
units of:

936. a full custom digital signal processing (DSP) unit
which can be supplemented with silicon compiler hardware
circuitry for Reed-Solomon (RS) parity decoding for transmission
line errors, with hardware circuitry for IBM's patented Data
Encryption Standard (DES) decryption only in 'canned data' use
for conversion of 'cipher-text' streaming media into 'plain
text,' with silicon compiler circuitry for doing MPEG X de-
compression (1/ 2 CODEC) for high data rate 'canned data.' The
prior art DSP unit itself is mostly used for byte shuffling
around the "back-side DSP bus" and also for custom firmware
digital signal processing (DSP) such as artificial digital signal
degradation algorithms (data lost can never be re-gained by
hackers).

940. an inter-function on-chip back-side input/output

(I/O) bus,

942. a first in first out buffer (FIFO)

with an I/O port latched access on the I/O bus

943. to front-side memory/data bus

944. controller circuitry such as a bus interface unit

(BIU), counter timer circuitry (CTC), memory access (RAS/CAS) and refresh strobe (DMA) logic, direct memory access circuitry (DMA), interrupt controllers, etc,

948. static RAM (SRAM) or dynamic RAM (DRAM) for temporary data store,

952. cryptographic memory which can be tamper resistant

non-volatile electrically erasable programmable read-only memory (TNV-EEPROM) for non-volatile cryptographic program store and cryptographic data store,

960. an around the chip metal deposition layer mask for

tamper detection using impedance measuring which will erase the cryptographic memory upon tamper detection,

964. built-in block oriented error detection and

correction circuitry such as Reed-Solomon (RS) parity coding (very important for block oriented decryption modes which use block chaining which can also chain errors across a message),

968. secret key hardware decryption only (executed before decompression to undo things in the proper order) which can be Data Encryption Standard (DES) in several modes such as Triple DES, block cipher modes of electronic codebook (ECB) and cipher block chaining (CBC), and also stream cipher modes of cipher feed-back (CFB) and output feed-back (OFB),

972. a MPEG X one-half video CODEC of decompression only,

976. RAM digital to analog converters (RAMDAC's) with optional artificial digital signal degradation units (anti-piracy technique) to produce modulated digital red, green, blue (modulated digital RGB) output for a digital monitor, or else analog output for existing analog audio/video televisions such as NTSC (US and Japan), PAL (UK and colonies), or SECAM (French and colonies).

980. analog video line amplifiers,

984. a MPEG X one-half audio CODEC of decompression only to various audio formats such as digital 2-channel stereo, digital theater type 5.1 speaker sound (e.g. Dolby surround sound (AC3)), or even full commercial theater 30 channel sound,

988. audio digital to analog converters (DAC's) with optional artificial digital signal degradation units (anti-piracy technique) to produce analog sound for loud-speakers,

992. analog audio line amplifiers,

993. (optional) n-dimensional digital timing and digital signal outputs such as for seat vibration effects, olfactory unit effects, automatic theater drapery controls, automatic theater lighting controls, timing cues for local advertising inserts during intermissions, etc.,

1000. internal cryptographic media players future patent pending [REF 508] with embedded custom cryptographic digital signal processor units (932) [REF 500],

e.g. cryptographic PCI bus audio cards,

e.g. cryptographic PCI bus video cards,

e.g. cryptographic AGP port video cards,

personal computer (PC) must have a media ticket smart card reader, and computer keyboard.

1004. external cryptographic audio/video media players
future patent pending [REF 508] with built-in cryptographic
digital signal processor units (932):

e.g. cryptographic digital versatile disk read/write
players (C-DVD-RW, C-DVD+RW) players,

e.g. cryptographic compact disk record once players (C-
CD-R),

1008. has a built-in media ticket smart card reader,

1012. has a built-in toggle field with liquid crystal display
(LCD) for up to 10 alpha-numeric characters for
passphrase/passcode entry and also,

1016. has built-in toggle up/down and right/left control
buttons,

1020. (future option) has a built-in bio-identification
unit such as a digital fingerprint reader.

1040. external cryptographic audio media players future
patent pending [REF 508] with built-in cryptographic digital
signal processor units (932):

e.g. cryptographic moving picture electronics group
compression standard I Audio Layer 3 (MP3) players (audio
only), or else the use of newer Advanced Audio CODEC (R)
(AAC) using fast wavelet compression instead of the older
discrete cosine transform.

e.g. future versions of moving picture electronics
group compression standard I audio layer 3 (MP3) players
(audio only),

e.g. future versions of audio compression level 3
(AC3) (R) players (audio only) (this is a Dolby Labs (R)
standard called Dolby Digital Sound (R) for various format
recorded digitally compressed n-channel digitally
decompressed from 2-channel to 5.1-channel output digital
audio) for home use only,

1044. has a built-in media ticket smart card reader,

1048. has a built-in toggle field with liquid crystal
display (LCD) for up to 10 alpha-numeric characters,

1052. has built-in toggle up/down and toggle right/left
control buttons,

1056. (future option) has a built-in bio-identification
unit such as a fingerprint reader to read digital fingerprints.

1060. external cryptographic electronic book, electronic newspaper, video only media players future patent pending [REF 508] with a built-in cryptographic digital signal processor unit (932):

e.g. cryptographic digital versatile disk
read/write players (DVD-RW, DVD+RW) players,

e.g. cryptographic compact disk record once players
(CD-R) has a built-in media ticket smart card reader,

1064. has a built-in toggle field with liquid crystal display (LCD) for up to 10 alpha-numeric characters,

1068. has built-in toggle up/down and toggle right/left
built-in control buttons,

1072. (future option) has a built-in bio-identification unit
such as a digital fingerprint reader.

1200. digital television monitors (like a computer monitor)
taking modulated digital red, green, blue (RGB) signals which
need a set-top box converter. A digital television has a built-
in set-top box for some type of digital audio/video input signal.

DETAILED DESCRIPTION OF INVENTION - Detailed Description of Drawings -
Preferred Embodiment:

Fig. 1 is a pyramid showing the layered design of the full proposed cryptographic system and where the media ticket smart card and custom digital media distribution public key cryptography architecture is suggested as an embodiment.

Fig. 2 is a circuit block diagram of a prior art cryptographic microprocessor unit found in a prior art smart card.

Fig. 3 is a circuit block diagram of a prior art media ticket smart card (212). This is used for secret key and private key secure containment and physical transportation.

Fig. 4 is a circuit block diagram of a prior art media ticket smart card reader attached to a personal computer.

Fig. 5 is a circuit block diagram of a cryptographic digital signal processor (C-DSP) (932) [REF 500]. This is used for doing hybrid key cryptography which is both public key cryptography and fast hardware based secret key cryptography inside of a digital signal processor processing digital signals in a cryptographically secure environment.

Fig. 6 is a circuit block diagram of a cryptographic media player [REF 508] with a built-in media ticket smart card reader.

Fig. 7 is a unit block diagram of the 1st alternative embodiment of a universal input cryptographic set-top box for encrypted or "cipher text" high definition television (HDTV)/standard definition television (SDTV) signals coming "over the airwaves", by cable system, by phone system, by satellite, or by IEEE 802.11c wireless Ethernet connections.

Fig. 8 is a circuit block diagram of the 1st alternative embodiment of a universal input cryptographic set-top box for encrypted or "cipher text" high definition television (HDTV)/standard definition television (SDTV) signals coming "over the airwaves", by cable system, by phone system, by satellite, or by IEEE 802.11c wireless Ethernet connections.

Fig. 9 is a circuit block diagram of the 2nd alternative embodiment of a cryptographic micro mirror module (MMM) commercial movie theater system.

DETAILED DESCRIPTION OF INVENTION - Operation of Invention - Preferred Embodiment

Fig. 1 is a pyramid showing the layered design of the proposed new type of cryptographic system and where the media ticket smart card and custom digital media distribution cryptography architecture is suggested as an embodiment.

Definition of trusted ("black") hardware.

Cryptographic keys can only be held in trusted hardware which is equipped with tamper resistant non-volatile electrically erasable programmable read only memory (TNV-EEPROM). This is prior art tamper detect and tamper erase memory using a metal interconnect to detect pin port probers through impedance monitoring which is integrated with prior art integrated circuitry.

Cryptographic keys even in secret key encrypted form mixed with random noise called "salt" should absolutely never be held in any non-cryptographic memory such as prior art computer hard disks for permanent storage!!!!!!!!!!

Non-cryptographic permanent memory examples are ordinary prior art hard disk drives, compact disk record once drives, digital versatile disk read/write drives, or flash (bank programmable) types of solid state memory card drives.

Unencrypted digital masters represent multi-million dollar sources of piracy revenue and are considered a media distribution company's jealously guarded crown jewels. The compromising of cryptographic keys will release multi-million dollar digital masters of hit movies and hit music to the illegal pirate or bootleg video and music industry. Record company promotional pre-releases of music and movie company first release movie masters are routinely copied by illegal

copyright pirates even before the first commercial releases to the public!!!!

The media distribution company's secure world wide web server is assumed to be secure and trusted being physically guarded at the media distribution company's central office building and also with internet gateway firewall protection. Various Web security domains can exist within the same physically secured office with different levels of controlled physical access. Web server security levels are from highest to lowest:

A). For highest security, the web server may be an isolated server with no or extremely restricted local area network office connections which holds no unencrypted digital media masters, only encrypted digital media masters. Footprint downloads or data transfer must occur from the ordinary office local area network using hand carried removable hard disk drives and streaming tape cassettes.

B). For the medium security server, the web server may be a proxy server (network protocol isolation server) or have local area network protocol isolation with the rest of the office. No other office phone lines or modem connections or Wide Area Network lines should be allowed to avoid points of hacker entry. Only the single World Wide Web Internet server line to the outside world should exist. The server should have a firewall for protection from the outside world.

C). For the lowest security server, the web server has a local area network connection to the office. Absolutely no outside phone lines or modem connections or Wide Area Network lines are allowed. Only the single World Wide Web Internet server line to the outside world should exist. The server should have a firewall for protection from the outside world.

The only secure tamper resistant non-volatile electrically erasable programmable read only memory (TNV-EEPROM) or shortened to secure cryptographic memory available in this system is:

A). in the media ticket smart card

B). in the cryptographic media player [REF 508] or more specifically inside of its cryptographic digital signal processor integrated circuit chip (e.g. crypto-MP3 player).

Definition of untrusted ("red") hardware.

The internet is untrusted hardware.

Any non-cryptographic memory is untrusted hardware.

Any non-cryptographic memory devices are untrusted hardware.

Any wiretappable buses are untrusted hardware.

Pass-thru encryption of cryptographic keys using family keys upon unencrypted data always combined with sequence numbers or time stamps if a clock is available upon both sides to prevent recorded replay attacks must be done over all untrusted ("red") hardware and buses.

Any secure sockets layer (SSL) internet connection is considered to be untrusted hardware!!!!!!

It is definitely not secure enough for transporting cryptographic keys which could be used by pirates to illegally access the clear-text (unencrypted) digital masters of multi-million dollar, commercial digital media such as hit movies, hit music, electronic newspapers, and popular electronic format books. This is because a fully automated hacker personal computer program which can be remotely planted by a virus will automatically extract secure sockets layer private keys and secret keys from hard disks. Such a hacker program will eventually be produced by hackers if indeed it does not already exist because there are no technological barriers to stop the hacker. The hackers will use assembly code dis-assembly and logic analyzers to reverse engineer the assembly code location and secret key encryption algorithm which mixes the private key and secret key with random noise called "salt" and permanently stores the private key and secret keys on hard disk.

A hacker program will be made to automatically retrieve the secret key encrypted private key and secret keys on hard disk and then randomly try to brute force crack the correct key sequence.

Alternately, a simple keyboard capture buffer remotely planted by a virus can retrieve the keyboard entered customer password and also find out the operating system secret key used to encrypt the private key stored on hard disk for permanent storage.

Media Ticket Smart Card System Authority and

Vendor Factory Pre-Distribution

Activities

Factory distribution of cryptographic keys (before any internet based media distribution)..

The media ticket smart card system authority, party S, has a division of powers into three components to keep the potential access to plain text digital masters restricted to the originating digital media distribution company (its crown jewels worth multi-millions of dollars):

A). public key generating authority (PuKGA), party G: has knowledge of whole private keys and whole family keys, but, no knowledge of customer identifications of any kind.

B). public key distribution authority (PuKDA), party D: has knowlege of customer identifications of the kind registered by customers through retail store forms, web registration, and mail-back postcards, but, no knowledge of whole private keys and whole family keys.

C). public key escrow authorities (PuKEA), parties En (a minimum of parties E1 and E2 for cryptographic keys split into a front-half and a back-half):

party E1 has only half of private keys,

half of family keys, half of secret keys.

party E2 has the other halves.

party E1 and party E2 have no

customer identification information of any kind.

Central Public Key Generation Authority

(PuKGA) - Party G

The media ticket smart card system authority, party S, has a dedicated function of a public key generation authority, party G:

which has knowledge of whole cryptographic keys, but, no knowledge of customer identities or vendor identities!!!!!!

A). Input to PuKGA:

None.

B). Processing by PuKGA:

1). Party G generates from true random noise: the system family key (FaK-F) which is a family key (common secret key (SeK-F)), FaK-F, where party F is the common family, which is given to the public key distribution authority, party D, for eventual pre-factory distribution to trusted media distribution companies, party Vn.

2). Party G generates an initialization vector (IV) used as a secret key seed (SeK-D) given only to:

a). the public key generation authority (C-PuKGA), party G,

b). the public key distribution authority (C-PuKDA), party D,

The top secret initialization vector (IV) is used as the seed for a message authentication cipher (MAC). A message authentication

cipher (MAC) is a message digest cipher (MDC) using a secret seed which restricts its use to classified parties. A message digest cipher (MDC) is a one-way hash code which in example inputs a 512-bit cipher block of data and produces a fixed bit output uniquely representing the data such as a 128-bit pseudorandom output. A message authentication cipher (MAC) code (MAC code) is a fixed bit output such as 128-bits uniquely representing some digital data which only the holders of the initialization vector (IV) can produce.

3). The initialization vector (IV) is distributed by the party G only to the central public key distribution authority (C-PukDA), party D, who will use it to keep the customer index number (CIN) top secret to stop its use to link cryptographic keys to owners (just as social security numbers should be kept citizen secret). Instead of a customer index number (CIN), a message authentication cipher code (MAC code) of the customer index number (CIN) is made public called the MAC(CIN).

4). The public key generation authority, party G, pre-factory prepares media ticket smart cards:

a). The public key generation authority, party G, pre-factory deposits a family key, FaK-F, copy into every blank media ticket smart card before they are given to the public key distribution authority, party D, for eventual physical distribution to trusted media distribution companies, parties Vn, who in turn will factory

distribute them to customers at retail stores and in the certified mail.

b). The party G will generate an incremented customer index number (CIN) which is kept top secret.

c). The party G will compute a message authentication cipher (MAC) of the customer index number (CIN) called the MAC(CIN) which is used as a public customer identification number.

d). Party G pre-factory generates public key/private key pairs with the private key always being kept top secret and the public key as public information,

{PrK-A, PuK-A},

{PrK-B, PuK-B},

etc.

for all customers, party A, party B, etc. and assigns them one by one to customers of unknown identity:

{CIN, MAC(CIN), PrK-A, PuK-A},

{CIN, MAC(CIN), PrK-B, PuK-B},

etc.

e). Party G pre-factory embeds into media ticket smart card A, the values of:

G-FaK-F

{-----, MAC(CIN), PrK-A, PuK-A}

and into media ticket smart card B, the values of:

G-FaK-F

{-----, MAC(CIN), PrK-B, PuK-B}

etc.

and imprints on the smart card exterior the public customer identification number, MAC(CIN), for identification, since, the central public key distribution authority (C-PuKDA), party D will have no access to the public keys or private keys inside.

Access to the private key field of the media ticket smart cards will be done through an access code (e.g. passphrase/passcode, or password with vowels substituted by pseudo-random noise) which initial access code must be denied the Central public key Distribution Authority (C-PuKDA), party D, who can have no knowledge of private keys. Therefore, the initial access code is stored inside of a party G database given to a public key access code authority

(PuKAC) who will later contact the customer with the initial access code:

```
{  
  
    {-----, MAC(CIN), -----, PuK-A,  
  
    initial access code},  
  
    {-----, MAC(CIN), -----, PuK-B,  
  
    initial access code},  
  
    etc.  
  
}
```

f). Party G gives the media ticket smart cards to the party D who in turn will give them to authorized media distribution companies, parties Vn, for eventual sale to customers.

h). The party G gives a customer public key database without private keys to the central public key distribution authority (C-PuKDA), party D, for eventual publishing on the world wide web (WWW):

```
{CIN, MAC(CIN), -----, PuK-A},  
  
{CIN, MAC(CIN), -----, PuK-B},  
  
etc.
```


The party D will make all public keys without private keys or customer index number (CIN) publicly available over a media ticket smart card system authority internet web server using digital certificate standards (e.g. International Telegraphy Union's (ITU's) X.509 standard).

{---, MAC(CIN), -----, PuK-A,

customer name, etc.},

{---, MAC(CIN), -----, PuK-B,

customer name, etc.},

This new method does not trust other public key systems already in use!!!!!!!!!! Existing public key systems such as secure sockets layer (SSL) based public keys are not hacker safe and may be compromised which would give away multi-million dollar in value commercial digital masters for music and movies!!!!!!!!

i). The public key generation authority, party G, may destroy the private keys after smart card depositing for absolute privacy. The private keys are kept top secret.

j). Optionally the party G may use a central public key escrow authority (C-PuKEA), parties En, with a minimum of two escrow parties to hold the front half and the back half of split cryptographic keys, to hold split cryptographic keys.

{---, MAC(CIN), key split PrK-A, PuK-A},

{---, MAC(CIN), key split PrK-B, PuK-B},

etc.

5). The public key generation authority (C-PuKGA), party G, pre-factory prepares the cryptographic digital signal processors (C-DSP) for transfer to the public key distribution authority (C-PuKDA), party D, for passing to the media distribution vendors, parties Vn, for eventual manufacturing into cryptographic media players [REF 508] for customer sale.

a). Party G pre-factory prepares the cryptographic digital signal processing (C-DSP) integrated circuits eventually used inside of the cryptographic media players [REF 508] by hardware manufacturers.

b). Party G must pre-factory install cryptographic keys into the tamper resistant non-volatile electrically erasable programmable read only memory (TNV-EEPROM) of the cryptographic digital signal processing (C-DSP) integrated circuits (IC's).

A cryptographic digital signal processing unit (C-DSP) includes:

cryptographic memory for crypto keys and crypto algorithms,

hardware session key (1-time secret keys)

decryption circuits with hardware block error detection and correction,

MPEG X digital decompression circuits (in players only a

Digital MPEG X de-compression only device called a 1 /2 CODEC with the compression part missing),

digital audio/video signal processing circuits,

digital artificial signal degradation circuitry,

analog audio/video or analog signal processing circuits with line amplifiers for output to loudspeakers,

digital video signal modulation to analog for modulated digital output to computer monitor displays (e.g. SVGA monitors, UXGA monitors, etc.)

c). Party G installs the media ticket smart card system authority system family key, called party F, FaK-F into the cryptographic digital signal processors (C-DSP's).

d). Party G generates a top secret vendor index number (VIN) for all media distribution vendors, parties Vn. Party G also generates a public vendor identification number using a message authentication cipher of vendor index number (MAC(VIN)).

e). Party G generates vendor private key/public key pairs:

{VIN, MAC(VIN), PrK-Vn, PuK-Vn},

{VIN, MAC(VIN), PrK-Vn, PuK-Vn},

etc.

The whole set of unique vendor private keys, PrK-Vn, and public keys, PuK-Vn, indexed by vendor identification number (MAC(VIN)) will be embedded into each and every cryptographic digital signal processor for eventual use in cryptographic media players which are isolated in network use although a local "red" communications channel with a customer inserted media ticket smart card is supported:

{---, MAC(VIN), PrK-Vn, PuK-Vn},

{---, MAC(VIN), PrK-Vn, PuK-Vn},

etc.

f). Party G will distribute to the central public key distribution authority (C-PuKDA), party D:

{VIN, MAC(VIN), -----, PuK-Vn},

{VIN, MAC(VIN), -----, PuK-Vn},

etc.

Party D will distribute to each vendor, party Vn, only his own public key data including his own top secret vendor private key, PrK-Vn:

{VIN, MAC(VIN), PrK-Vn, PuK-Vn}

g). The public key generation authority, party G, may destroy the vendor private keys, PrK-Vn, after cryptographic digital signal processor depositing for absolute privacy. The private keys are kept top secret to each vendor.

h). Optionally the party G may use a central public key escrow authority (C-PuKEA), parties En, with a minimum of two escrow parties to hold the front half and the back half of split cryptographic keys, to hold split cryptographic keys.

{---, MAC(VIN), key split PrK-Vn, PuK-Vn},

{---, MAC(VIN), key split PrK-Vn, PuK-Vn},

etc.

6). Party G will also generate unique to each media distribution vendor, party Vn, a unique vendor secret key, SeK-Vn. Party G will give this vendor secret key to the central public key distribution authority for eventual distribution to each media distribution vendor of only his own top secret vendor private key which protects his own digital media masters.

{VIN, MAC(VIN), -----, SeK-Vn},

{VIN, MAC(VIN), -----, SeK-Vn},

etc.

7). Party G will embed the whole set of unique vendor secret keys, SeK-Vn, indexed by vendor identification number (MAC(VIN)) into each and every cryptographic digital signal processor (C-DSP) for eventual manufacturing into cryptographic media players.

{VIN, MAC(VIN), -----, SeK-Vn},

{VIN, MAC(VIN), -----, SeK-Vn},

etc.

8). The public key generation authority, party G, may destroy the vendor secret keys, SeK-Vn, after cryptographic digital signal processor depositing for absolute privacy. The private keys are kept top secret.

9). Optionally the party G may use a central public key escrow authority (C-PuKEA), parties En, with a minimum of two escrow parties to hold the front half and the back half of split cryptographic keys, to hold split cryptographic keys.

{---, MAC(VIN), key split SeK-Vn},

{---, MAC(VIN), key split SeK-Vn},

etc.

10). Party G gives the programmed cryptographic digital signal processing integrated circuits (IC's) to the central distribution authority (C-PuKDA), party D, who will pass them to the media distribution vendors, parties Vn, for factory manufacture into cryptographic media players.

11). The public key generation authority (C-PuKGA), party G, may deposit important split cryptographic keys with the central public key escrow authority (C-PuKEA), parties En:

Optionally, the media ticket smart card system authority - public key generation authority function may key split the cryptographic keys as into a front half and a back half and transfer the cryptographic keys to at least two separate public key escrow authorities. The public key escrow authority function handles the cases of customer lost media ticket smart cards or customer stolen media ticket smart cards or disputes over legal ownership of media ticket smart cards as in divorce cases. This key escrow function allows the media ticket smart card system authority to re-construct

cryptographic data and cryptographic keys after lost or stolen media ticket smart cards are reported which might otherwise represent data permanently lost to customers. Disputed legal ownership of media ticket smart cards as in divorce or separation cases may also restore media ticket smart card contents to rightful legal owners even if the smart card itself is not available to a court.

The cryptographic keys should be key split into at least a front half key and a back half key just like breaking it in half. The front half of all keys generated and issued is deposited by the media ticket smart card system authority with a neutral key escrow agent in a computer relational database. The back half of all keys generated and issued is deposited by the media ticket smart card system authority with an entirely separate neutral key escrow agent in a computer relational database.

It is assumed for convenience, payment, and legal ownership that each customer will usually have only one registered media ticket smart card registered with the media ticket smart card system authority for all of his own personal music and movies.

Party E1 receives (front key split halves of):

Customer private key pairs:

(

{---, MAC(CIN), front half PrK-A, PuK-A),

{---, MAC(CIN), front half PrK-B, PuK-B),

etc.

}).

Vendor private key, PrK-Vn, pairs:

```
{  
  
  {---, MAC(VIN), front half PrK-Vn},  
  
  {---, MAC(VIN), front half PrK-Vn},  
  
  etc.  
  
}
```

Vendor unique secret key, SeK-Vn, pairs:

```
{  
  
  {---, MAC(VIN), front half SeK-Vn},  
  
  {---, MAC(VIN), front half SeK-Vn},  
  
  etc.  
  
}
```

Party E2 receives (back key split halves of):

Customer private key pairs:

```
(  
  
  {---, MAC(CIN), back half PrK-A, PuK-A},  
  
  {---, MAC(CIN), back half PrK-A, PuK-A},  
  
  etc.  
  
)
```

Vendor private key, PrK-Vn, pairs:

```
{  
  
  {---, MAC(VIN), back half PrK-Vn},  
  
  {---, MAC(VIN), back half PrK-Vn},  
  
  etc.  
  
}
```

Vendor unique secret key, SeK-Vn, pairs:

```
{  
  
  {---, MAC(VIN), back half SeK-Vn},  
  
  {---, MAC(VIN), back half SeK-Vn},  
  
  etc.  
  
}
```

Central Public Key Distribution Authority

(C-PuKDA) - Party D

The media ticket smart card system authority, party S, has a dedicated function of a central public key distribution authority (C-PuKDA), party D:

which has knowledge of customer identifications and vendor identifications, but, no knowledge of whole cryptographic keys!!!!

A). Input to C-PuKDA, party D:

1). Party D receives from the central public key generation authority (C-PuKGA), party G, the following:

2). Party D receives from party G who generates from true random noise: the system family key (FaK-F)

which is a common secret keys (SeK-F) where party F is the common family, which is given to the public key distribution authority, party D, for eventual pre-factory distribution to trusted media distribution companies, party Vn.

3). Party D receives from party G, the initialization vector (IV). Party D will use it to keep the customer index number (CIN) top secret to stop its use to link cryptographic keys to owners (just as social security numbers should be kept citizen secret).

Instead of a customer index number (CIN), a message authentication cipher code (MAC code) of the customer index number (CIN) is made public called the MAC(CIN).

4). Party D will receive from party G a customer public key database without private keys to the central public key distribution authority (C-PuKDA), party D, for eventual publishing on the world wide web (WWW) without the top secret customer index number (CIN):

{CIN, MAC(CIN), -----, PuK-A},

{CIN, MAC(CIN), -----, PuK-B},

etc.

5). Party D receives from party G the pre-factory programmed media ticket smart cards who in turn will give them to authorized media distribution companies, parties Vn, for eventual sale to customers.

6). Party D receives from party G media distribution vendor databases:

{VIN, MAC(VIN), -----, PuK-Vn},

{VIN, MAC(VIN), -----, PuK-Vn},

etc.

7). Party D will distribute to each vendor, party Vn, only his own public key data:

{VIN, MAC(VIN), -----, PuK-Vn}

8). Party D receives from party G who will also generate unique to each media distribution vendor, party Vn, a unique vendor secret key, SeK-Vn. Party G will give this vendor secret key to the central public key distribution authority for eventual distribution to each media distribution vendor.

{VIN, MAC(VIN), -----, SeK-Vn},

{VIN, MAC(VIN), -----, SeK-Vn},

etc.

9). Party D receives from party G who will embed the whole set of unique vendor secret keys, SeK-Vn, for every party Vn into each and every cryptographic digital signal processor (C-DSP) for eventual manufacturing into cryptographic media players.

{VIN, MAC(VIN), -----, SeK-Vn},

{VIN, MAC(VIN), -----, SeK-Vn},

etc.

10). Party D receives from party G the pre-factory programmed cryptographic digital signal processor integrated circuits and party D will in turn distribute the chips to the media distribution

companies, parties Vn, for manufacturing into cryptographic media players and for further factory use and eventual customer distribution at retail stores.

B). Processing by C-PuKDA:

1). Party D keeps a top secret computer database record of:

{

authorized media distribution vendor index number (top
secret) (VIN),

public vendor identification number = message
authentication cipher (MAC) of vendor index number
(MAC(VIN)),

{---,

MAC(CIN),

-----,

PuK-n,

eventual registered customer name

(by retail store registered, Web registered, or
registration postcard, or media distribution vendor
database updates)

},

}

2). Party D, look-up of customer name in this top secret database will give the top secret customer index number (CIN). Use of the message authentication cipher (MAC) seeded with the initialization vector (IV) upon the customer index number (CIN) will produce a message authentication cipher code (MAC code) which can be handed to the central public key escrow authorities, parties En, to retrieve key split cryptographic keys and family keys and also used to index the initial media ticket smart card access code database held by the Central public key Access Code Authority (C-PuKAC), party EA for mailing or transmitting the initial access code to customers.

3). Party D keeps a top secret computer database record of:

{

{VIN,

MAC(VIN),

-----,

PuK-Vn,

-----,

vendor identification such as name, address,

etc.

},

}

C). Output of C-PuKDA:

1). Party D pre-factory distributes the media ticket smart card system authority system family key, FaK-F, to the media distribution companies, parties Vn.

2). Party D gives the programmed cryptographic digital signal processing (DSP) integrated circuits to the authorized media distribution vendors who will factory manufacture them into cryptographic media players.

3). Party D distributes to each media distribution vendor, Vn, his own, unique secret key (SeK-Vn). Party G has already key split these secret keys for deposit with the neutral, key escrow parties, party E1 and party E2.

4). Party D distributes to each media distribution vendor, Vn, his own, unique vendor private key (PrK-Vn) with a message authentication cipher of vendor identification number (MAC(VIN)). Party G has already key split these secret keys for deposit with the neutral, key escrow parties, party E1 and E2.

5). Party D distributes to each media distribution vendor, Vn, his plain text vendor identification number which consists of the message authentication cipher of the vendor index number (MAC(VIN)) (for

system family key encryption and download with encrypted media to customers to identify the vendor).

6). Party D publishes the customer public key database for use by the media distribution vendors, Vn:

{---, MAC(CIN), -----, PuK-A},

{---, MAC(CIN), -----, PuK-B},

etc.

7). Party D gives to the Central Public Key Access Code Authority (C-PuKAC), Party EA, a top secret computer database record to help in mailing initial access codes to customers of:

{

-----,

public media distribution vendor

identification = message authentication cipher (MAC) of
vendor index number MAC(VIN),

{---,

MAC(CIN),

-----,

PuK-n,

eventual registered customer name (retail store
registered, Web registered, or registration postcard)

},

}

Central Public Key Escrow Authorities

(C-PuKEA) - Parties En

The media ticket smart card system authority, party S, has a dedicated function of a central public key escrow authority (C-PuKEA), parties En:

which has knowledge of split cryptographic keys, but, no knowledge of whole cryptographic keys, customer identifications and vendor identifications!!!!

A). Input to C-PuKEA:

1). The parties En may optionally receive from the party G (with a minimum of two escrow parties to hold the front half and the back half of split cryptographic keys, to hold split cryptographic keys):

{---, MAC(CIN), key split PrK-A, PuK-A},

{---, MAC(CIN), key split PrK-B, PuK-B},

etc.

2). The parties En may optionally receive from the party G (with a minimum of two escrow parties to hold the front half and the back half of split cryptographic keys, to hold split cryptographic keys):

{---, MAC(VIN), key split PrK-Vn, PuK-Vn},

{---, MAC(VIN), key split PrK-Vn, PuK-Vn},

etc.

3). The parties En may optionally receive from the party G (with a minimum of two escrow parties to hold the front half and the back half of split cryptographic keys, to hold split cryptographic keys):

{---, MAC(VIN), key split SeK-Vn},

{---, MAC(VIN), key split SeK-Vn},

etc.

B). Processing by C-PuKEA:

1). An independent function of the media ticket smart card system authority (C-PuKEA), party S, is the central public key escrow authorities, parties En (a minimum of parties E1 and E2),

2). This authority takes care of customer lost, stolen, and legally disputed media ticket smart cards.

Party E1 receives (front key split halves of):

key split media ticket smart card system family key (FaK-F),

key split initialization vector (IV) used as a secret key
(SeK) for the message authentication cipher (MAC) used upon the
top secret, customer index number (CIN).

(whole message authentication cipher code of customer index
number (MAC(CIN))),

key split public key pair n (PuK-n, N),

key split private key pair n (PrK-n, N)).

3). Party E2 receives (back key split halves of):

key split media ticket smart card system family key (FaK-F),

key split initialization vector (IV) used as a secret key
(SeK) for the message authentication cipher (MAC) used upon the
top secret, customer index number (CIN).

(public customer identification code = whole message
authentication cipher (MAC) code of customer index number
(MAC(CIN))),

key split public key pair n (PuK-n, N),

key split private key pair n (PrK-n, N)).

4). Customer media ticket smart cards which are lost, stolen, or of disputed legal ownership must be handled to preserve use of custom, encrypted digital media still in customer ownership. This is initiated by customers, party A, contacting the central public key distribution authority (C-PuKDA), party D who in turn will contact the parties En using the public customer identification number or MAC(CIN) to retrieve split cryptographic customer keys.

C). Output by C-PuKEA:

None.

Central Public Key Access Code Authorities

(C-PuKAC) - Parties EAn

The media ticket smart card system authority, party S, has a dedicated function of a central public key access code authority (C-PuKAC), parties EAn:

which has knowledge of media ticket smart card initial access codes and customer identifications in order to mail initial access codes to customers, but, has absolutely no access to media ticket smart cards and no knowledge of whole cryptographic keys!!!!

A). Input to C-PuKAC:

1). Party EA receives from the central public key generation authority (C-PuKGA), party G, the initial access code database.

{

{-----, MAC(CIN), -----, PuK-A,

initial access code},

{-----, MAC(CIN), -----, PuK-B,

initial access code},

etc.

}

}

2). Party EA receives from the Central Public Key Distribution Authority (C-PuKDA), Party D, a top secret computer database record to help in mailing initial access codes to customers of:

{

authorized media distribution vendor id (VIN),

{---,

public customer identification number

(MAC(CIN)),

-----,

customer n's public key (PuK-n),

eventual registered customer name

(retail store registered, Web registered, or registration postcard)

},

}

B). Processing by C-PuKAC:

1). The public key access code authority (PuKAC), party EA, will later mail in secure certified mail or transmit over secure sockets layer (SSL) to each customer his own initial access code. The initial access code gives customer access to use of his private key field and does not compromise session keys or digital masters.

C). Output by C-PuKAC:

None.

Authorized Media Distribution Vendors -

Parties Vn

The authorized media distribution vendors, parties Vn:

which have no knowledge of whole customer cryptographic keys,
but, have knowledge of customer identifications!!!!

A cryptographic algebra notation implemented in the central media world wide web (WWW) server, party Vn (distribution), for each customer, party A, party B, party C, party E (reserved for key escrow

companies), party F (reserved for the common secret family key), party G, party H, etc. is as follows:

A). Input to Vn:

1). Party Vn receives from the public key distribution authority (C-PuKDA), party D, pre-factory distributed cryptographic keys:

a). The distribution party, party Vn, the media ticket smart card used by the customer party A (unavailable to the customer himself in secure, tamper resistant, non-volatile, electrically erasable programmable read only memory (TNV-EEPROM), in short called cryptographic memory) has a pre-factory, party G installed system family key (FaK-F).

The cryptographic media player [REF 508] has a pre-existing, pre-factory, party G installed system family key (FaK-F) in cryptographic memory.

b). The media distribution company, Vn, has a party G, pre-factory distributed unique vendor secret key (SeK-Vn), stored in cryptographic memory.

Any authorized cryptographic media player [REF 508] also receives from party G an entire set of pre-factory distributed unique secret keys, SeK-V1 to Vn for all vendors stored in its cryptographic memory.

c). The media distribution company, Vn, has a party G, pre-factory distributed unique vendor private key (PrK-Vn), stored in cryptographic memory.

Any authorized cryptographic media player [REF 508] also receives from party G an entire set of pre-factory distributed unique public keys, PuK-V1 to Vn for all vendors stored in its cryptographic memory.

B). Processing by Vn:

1). The distribution party Vn's computation in his physically secure, media distribution company central office:

These following steps are done in a secure office computer with only a proxy server local area network connection to an internet server (hacker accessible) and also with no phone line access to protect the unencrypted digital masters.

a). The media distribution party, party Vn, uses his unique message authentication code (MAC) of vendor index number (MAC(VIN)) (the message authentication cipher is not known by the party Vn) as the public vendor identification number (MAC(VIN)) in order to download his public vendor identification number along with an incremented session id number to customers for indexing of the downloaded custom encrypted digital media and also cross-indexing

with the encrypted play code with header and encrypted play count
with header.

b). The custom encrypted digital media is defined as:

```
{  
  
vendor identification number MAC(VIN)),  
  
session id number,  
  
play code (SsK-A) encrypted digital media,  
  
}
```

c). The vendor and customer unique encrypted play code with header is defined as:

```
{  
  
{vendor identification number (MAC(VIN)),  
  
session id number,  
  
customer public key (PuK-A) encrypted  
  
{  
  
vendor secret key (SeK-Vn) encrypted  
  
{vendor digitally signed (PrK-Vn) {play code,  
  
vendor sequence number, MAC(CIN)}}},  
  
},  
  
customer (family key) sequence number,  
  
}},
```

d). The play code is defined as the session key (1-time secret key) used to custom encrypt the digital media.

e). The play count is defined as:

{

play count = paid for number of plays,

-1 for an infinite count, or

count of free trial plays.

}

f). The vendor and customer unique encrypted play count with header is defined as:

```
{

    {vendor identification number MAC(VIN)),

    session id number,

    customer public key (PuK-A) encrypted

    {

        vendor secret key (SeK-Vn) encrypted

        {vendor digitally signed (PrK-Vn) {play count,

        vendor sequence number}}

        -----,

        customer (family key) sequence number,

    }

}}
```

g). The two above steps of 1stly vendor secret key (SeK-Vn) encryption and 2ndly customer public key (PuK-A) encryption can be replaced by the almost equivalent in functionality but much slower steps of 1st customer public key (PuK-A) encryption and 2ndly

vendor public key (PuK-Vn) encryption (careful not to weaken the vendor digital signature). This assumes that a full set of vendor private keys (PrK-V1 to PrK-Vn) is contained in each cryptographic media player as well as the vendor public keys (PuK-V1 to PuK-Vn). The vendor public key decryption step is much slower than equivalent vendor secret key encryption step done in the cryptographic digital signal processor and will require revealing the vendor private keys to the cryptographic media player.

h). The media distribution vendor, Vn, uses his media ticket smart card system authority issued system family key, FaK-F, to family key pass-thru encrypt the encrypted play count with header, the encrypted play code with header all with sequence numbers to stop recorded replay attacks for download to the customer, party A.

$$Vn-FaK-F((\text{encrypted play count with header})) = V.$$

i). The media distribution vendor, party Vn, electronically web bills the customer, party A, over the internet to the prior art customer personal computer A by using credit card numbers transacted over a secure sockets layer (SSL) non-cryptographically secure transaction line.

j). Sequence numbers - The sequence numbers are needed to prevent recorded replay attacks on wiretappable buses of pass-thru encrypted signals inside of the cryptographic media player. The vendor sequence number can only be incremented by a party with the

vendor secret key (SeK-Vn), customer private key (PrK-n), and system family key (FaK-F) who are the party G for any vendor, the party Vn only for his own play codes and play counts, or the cryptographic media player, party P, for any vendor which player has a collection of all vendor secret keys (SeK-V1 to Vn) and a collection of all vendor private keys (PrK-V1 to Vn). Used in key ownership re-assignment operations by the C-DSP. The cryptographic media player, party P, can also check the vendor digital signature, and can obtain the customer A's private key (PrK-A) and public key (PuK-A) from customer's inserted media ticket smart card A. The customer (family key) sequence number is for media ticket smart card use only in loop-backed operations with the C-DSP.

k). The party Vn pass-thru encrypts the vendor and customer unique play count with header for transfer as:

system family key encrypted (Vn-FaK-F)

{

{vendor identification number MAC(VIN),

session id,

customer public key (PuK-A) encrypted

{

vendor secret key (SeK-Vn) encrypted

{vendor digitally signed (PrK-Vn) {play count,

vendor sequence number, MAC(CIN)}}

```

    },

    -----,

    customer (family key) sequence number,

}

}= V.

```

which is in cryptographic algebra short-hand notation:

```

Vn-FaK-F

(

MAC(VIN),

session id,

PuK-A(

SeK-Vn(

PrK-Vn(play count, vendor sequence number,

MAC(CIN)))),

customer (family key) sequence number,

)

```

1). The media distribution vendor, party Vn, uses a true random number generator to create a play code or session key (SsK-

A), for customer, party A. The session key is database recorded by party Vn, indexed by the public vendor identification number (MAC(VIN)) along with the digital media title downloaded and date and time.

```
{  
  
    vendor identification number (MAC(VIN)),  
  
    play code or session key (SsK-A),  
  
    customer A public key (PrK-A),  
  
    digital media title downloaded,  
  
    day of distribution,  
  
    month of distribution  
  
    year of distribution,  
  
    time of distribution,  
  
    -----,  
  
}
```

m). The media distribution company, party Vn, digitally signs the play code or session key (Vn-SsK-A), with its own top secret media distribution vendor private key (PrK-Vn), (this is not an encryption step because any holder of the public key (PuK-Vn) can de-scramble the session key):

$Vn-PrK-Vn(Vn-SsK-A, \text{ vendor sequence number}) = \text{temp-m}.$

n). The media distribution company, party Vn, wishes to keep this play code or session key (SsK-A), top secret from any customers and from any other vendors which will reveal his multi-million dollar digital masters to digital media competitors.

o). Party Vn also uses his top secret, unique, secret key (SeK-Vn), to encrypt (1st encryption) the result, temp-m, and an incremented sequence number to prevent recorded replay hacker attacks. A recorded replay hacker attack is a hacker who wiretaps open computer buses for digital recording and then simply re-introduces the value at a later time without ever decrypting it. Pass-thru encryption of fixed values is vulnerable to recorded replay hacker attacks.

p). Sequence Numbers - The sequence numbers are needed to prevent recorded replay attacks on wiretappable buses of pass-thru encrypted signals inside of the cryptographic media player. The vendor sequence number can only be incremented by a party with the vendor secret key (SeK-Vn), customer private key (PrK-n), and system family key (FaK-F) who are the party G for any vendor, the party Vn only for his own play codes and play counts, or the cryptographic media player, party P, for any vendor which player has a collection of all vendor secret keys (SeK-V1 to Vn) and a collection of all vendor private keys (PrK-V1 to Vn). Used in key ownership re-assignment operations by the C-DSP. The cryptographic media player, party P, can also check the vendor digital signature, and can obtain the customer A's private key (PrK-A) and public key (PuK-A) from customer's inserted media ticket smart card A. The customer (family key) sequence number is for use by the media ticket smart card in loop-back operations with the C-DSP.

q). The vendor's own secret key is shared only with the key escrow agents, parties E1 and E2, and a copy kept in the cryptographic media player [REF 508]:

$$Vn-SeK-Vn(temp-m) = temp-q.$$

r). The media distribution company, party Vn, can use the play code or unique session key, SsK-A, to uniquely encrypt only party A's digital media masters on the secure office computer which is inner firewall protected before proxy server transfer to a publicly (hacker) accessed internet (TCP/IP) protocol server or world wide web (WWW) server.

$Vn-SsK-A(\text{digital media})$

where:

$Vn-SsK-A(\text{data})$ means party Vn doing session key encryption using party A's play code or session key (1-time secret key) upon digital data.

s). The following steps can be done by using an inner firewall and proxy server local area network (LAN) connection to move the encrypted result X and also the uniquely encrypted digital media masters to a world wide web (WWW) server with an outer firewall.

2). 1-way transfer and custom session key encrypted media's unique session key (1-time secret key), SsK-A, used only for customer party A's digital medium. The following steps can be done by using an inner firewall protected proxy server local area network (LAN) connection to move the encrypted result, temp-q, and also the uniquely encrypted digital media masters through a firewall to a world wide web server with an outer firewall and anti-viral software updated weekly and run daily.

a). The media distribution company, party Vn, wishes to restrict this result X uniquely to customer A's media ticket smart card. Party Vn encrypts (2nd encryption) the result, temp-q, with the public key of Party A (PuK-A) which only Party A can decrypt with his private key A (PrK-A) stored inside of his media ticket smart card:

$$Vn-PuK-A(temp-q) = temp-s1.$$

b). The media distribution company, party Vn, wishes to restrict result, temp-s1, to trusted system parties. The media distribution company, party Vn, system family key (common secret key) to pass-thru encrypt (3rd encryption) the result, temp-S1, with the system family key, FaK, while careful not to pass-thru encrypt the result twice which will undo the pass-thru encryption:

```

Vn-FaK-F(

    MAC(VIN),

    session id number,

    temp-s1,

    customer (family key) sequence number,

    ) = temp-s2.

```

c). The summation, temp-s2, of these cryptographic operations becomes the pass-thru encrypted play code (session key):

pass-thru encrypted vendor and customer unique play code
with header =

```

family key pass-thru encrypted{

    {vendor indentification number (MAC(VIN))},

    session id,

    customer A public key encrypted

        {vendor secret key encrypted

            {vendor digitally signed {play code,

                vendor sequence number, MAC(CIN)}}},

```


}

customer (family key) sequence number,

}}

or in cryptographic algebra short-hand notation is:

Vn-FaK-F(

MAC(VIN),

session id,

PuK-A(

Vn-SeK-A

(Vn-PrK-Vn(Vn-SsK-A, vendor sequence no))

)

customer (family key) sequence number,

)

d). Sequence numbers - The sequence numbers are needed to prevent recorded replay attacks on wiretappable buses of pass-thru encrypted signals inside of the cryptographic media player. The vendor sequence number can only be incremented by a party with the vendor secret key (SeK-Vn), customer private key (PrK-n), and system family key (FaK-F) who are the party G for any vendor, the

party Vn only for his own play codes and play counts, or the cryptographic media player, party P, for any vendor which player has a collection of all vendor secret keys (SeK-V1 to Vn) and a collection of all vendor private keys (PrK-V1 to Vn). Used in key ownership re-assignment operations by the C-DSP. The cryptographic media player, party P, can also check the vendor digital signature, and can obtain the customer A's private key (PrK-A) and public key (PuK-A) from customer's inserted media ticket smart card A. The customer (family key) sequence number is for media ticket smart card use only for loop-back operations with the C-DSP.

The notation used is:

A-SeK-B(data) means party A doing secret key encryption using party B's secret key upon the clear text data.

SeK means a secret key

FaK means a family key (common secret key)

PuK means a public key

PrK means a private key

SsK means a session key (1-time secret key)

Party F is the family party or set of parties holding the family key (common secret key)

e). Establishment of a media header to help retrieve data from a customer, party A's, media ticket smart card.

Unique vendor and customer play count with header (and sequence numbers) is:

```
{  
  
    vendor indentification number (MAC(VIN)),  
  
    session id number,  
  
    customer public key (PuK-A) encrypted(  
        vendor secret key (SeK-Vn) encrypted  
        {vendor digitally signed (PuK-Vn)  
        {play count, vendor sequence number}},  
        _____),  
  
    customer (family key) sequence number,  
}
```

f). Unique vendor and customer play code with header (and sequence numbers) is:

```
{{vendor indentation number (MAC(VIN)),  
  
    session id number,  
  
    customer public key (PuK-A) encrypted{  
  
        vendor secret key (SeK-Vn) encrypted  
  
        {vendor digitally signed (PuK-Vn)  
  
            {play code, vendor sequence number}}},  
  
    customer (family key) sequence number,  
  
    }},
```

pair to download as an identification header at the start of custom encrypted digital media.

g). Followed by the custom encrypted digital media of:

```
{  
  
    vendor indentation number (MAC(VIN)),  
  
    session id number,  
  
    play code encrypted digital media,  
  
    [(Law Enforcement Access Field (LEAF) for law enforcement use  
    only using the embedded movie ticket concept):  
  
        public key courts {public key law enforcement  
  
            {
```

appended pass-thru encrypted play code plus

header,

vendor private key signed message digest cipher

(MDC)

}}

}

h). Media distribution vendor, Party Vn, internet world wide web (WWW) download of the encrypted play code with header and encrypted play count with header to the customer A's media ticket smart card A inserted into a media ticket smart card reader attached to his personal computer, followed by download of the custom encrypted digital media with legally forcing of an appended pass-thru encrypted play code with header which is downloaded to the customer A's physical digital media inserted into a drive on his personal computer.

i). Database records for each customer A, party A:

{

{vendor identification number (MAC(VIN)),

{customer identification of party A such

as name, address, etc.,

MAC(CIN),

PuK-A,

{date/time,

date, month, year,

title of digital media downloaded,

session id number,

customer unique play code or session key,

paid for amount,

},

{date/time,

date, month, year,

title of digital media downloaded,

session id number,

customer unique play code or session key,

paid for amount,

},

etc.

}

}

j). Only if a media ticket smart card is directly purchased and registered with the party Vn, a media distribution vendor database of customer identifications must be kept and updates sent to the central public key distribution authority (C-PuKDA) who will notify the central public key access code authority (C-PuKAC), party EA, such that party EA can certified mail or securely electronically transmit an initial media ticket smart card access code to the customer.

C). Output by Vn:

None.

Customers - Party A

The customers, party n, such as party A, party B, etc. (party D, E, F, G, P, S already in use) which have knowledge of customer identifications and vendor identifications and his own access code to a particular media ticket smart card for toggle field entry into a cryptographic media player in order to do "customer triangle authentication" of point 1: customer A, to point 2: smart card A, to point 3: trusted cryptographic player, but, no knowledge of whole cryptographic keys stored in cryptographic memory!!!!

Unique customer A, party A, completes several actions.

A). Input of Customer A:

1). Pick up at the retail store a cryptographic media player, a media ticket smart card, and registers the media ticket smart card indirectly with the media distribution vendor or else directly with the Central public key distribution authority (C-PuKDA), party D, giving his customer name, customer address, etc.

2). Receive from the central public key access code authority (C-PuKAC), party EA, his initial access code to the media ticket smart card which may be changed later.

B). Processing of Customer A:

Unique customer A, party A, upon every custom encrypted digital media download at his prior art world wide web (WWW) connected personal computer:

1). The system family key encrypted vendor identification number (MAC(VIN)), is downloaded to the customer A's personal computer and to his media ticket smart card (as part of the encrypted play code with header:

play code with header =

{

vendor identification number (MAC(VIN)),

session id,

various layers of the encrypted play code with

sequence number,

)

to ultimately identify the media vendor to the cryptographic media player.

2). This custom encrypted digital media data which is preceeded by a media identification header:

```

{

    vendor indentification number (MAC(VIN)),

    session id number,

    play code (session key or 1-time secret key)

        encrypted digital media,

        [(Law Enforcement Access Field (LEAF) for law enforcement
        use only using the embedded movie ticket concept which
        limits the divulging of cryptographic keys in key escrow
        unless for a high security inquiry reason always with a
        valid court order):

            public key courts {public key law enforcement

                {

                    appended pass-thru encrypted play code plus

                        header,

                            vendor private key signed message digest cipher

                                (MDC)

                                    }}

            }

}

```

This custom encrypted digital media with media header is internet world wide web downloaded by party Vn to party A's personal computer which transfers the encrypted digital media to a prior art personal computer's prior art peripheral drive containing either digital versatile disk read/write, or compact disk record once, or FLASH memory card. The unique encrypted

session key, SsK-A, is transferred through the personal computer media ticket smart card reader to an inserted media ticket smart card A.

3). The encrypted physical media and the smart card are transferred by party A to his cryptographic media player [REF 508].

Authorized Cryptographic Media Player - Party P

The authorized cryptographic media players, party P [REF 508]:

which have knowledge in cryptographic key memory of the system family key for pass thru encryption, all vendor public keys, and all vendor secret keys, but, no knowledge of customers or cryptographic media!!!!

4). A cryptographic algebra notation implemented in party A's cryptographic media player [REF 508] having a built-in media ticket smart card reader with party A's media ticket smart card inserted which plays the custom encrypted digital media using a cryptographic digital signal processor [REF 500] as follows:

a). the custom encrypted physical digital media is installed by customer A in his cryptographic digital media player (e.g. compact disk record once (CD-R), digital versatile disk read/write (DVD-RW, DVD+RW), flash bank programmable solid state memory cards (FLASH), digital cassette tape, etc.).

b). the customer A's own smart media A is installed into the built-in media ticket smart card reader in the cryptographic media player.

c). the cryptographic digital signal processor (C-DSP) in the cryptographic media player, party P, retrieves the plain text media header:

```
{  
  
    vendor indentification number (MAC(VIN)),  
  
    session id,  
  
    play code encrypted digital media,  
  
    [(Law Enforcement Access Field (LEAF) for law enforcement  
    use only using the embedded movie ticket concept):  
  
        public key courts {public key law enforcement  
  
            {  
  
                appended pass-thru encrypted play code plus  
  
                header,  
  
                vendor private key signed message digest cipher  
  
                (MDC)  
  
            }  
        }  
    }  
}
```

at the start of the media.

d). the cryptographic digital signal processor (C-DSP) in the cryptographic media player, party P, does customer triangle authentication to prevent use of lost or stolen media ticket smart cards from:

point 1, customer A (passphrase/passcode customer toggled into a built-in liquid crystal display (LCD) or else a more expensive and advanced bio-identification such as a digital fingerprint entered into a built-in fingerprint reader), to

point 2, media ticket smart card A (with play counts and play codes), to

point 3, trusted cryptographic media player.

Passphrase/passcode entry into a prior art computer keyboard or else a toggle field device with 1-line display such as a liquid crystal display (LCD) on the cryptographic media player [REF 508].

e). the cryptographic digital signal processor (C-DSP) in the cryptographic media player, party P, checks for the correct

physical custom encrypted media matched with the correct media ticket smart card by doing media triangle authentication:

point 1, custom encrypted media A, to

point 2, media ticket smart card A with paid
for encrypted play codes and encrypted play counts, to

point 3, authorized cryptographic media player.

f). the cryptographic digital signal processor (C-DSP) in the cryptographic media player, party P, retrieves using system family key pass-thru encryption with sequence numbers to avoid recorded replay hacker attacks, the party A's private key, PrK-A, from party

A's media ticket smart card A to its own tamper resistant memory. This should be the only private key on the media ticket smart card.

A more secure method which does not use a very vulnerable (not fully crypto memory contained) global vendor family key uses more media ticket smart card and more cryptographic digital signal processor cryptographic memory which is to use per vendor family keys, or alternately to use the vendor public key and vendor private key for replacing the global family key for smart card A to crypto-DSP transfers and visa versa with assorted details. The non-vendor specific hardware requirement forces storing crypto keys for all vendors in all cryptographic hardware memory.

g). the cryptographic digital signal processor (C-DSP) in the cryptographic media player, party P, retrieves the encrypted play count with customer (family key) sequence number to avoid recorded replay hacker attacks, from media ticket smart card A, and decrypts it. Where:

play count = paid for number of plays, or -1 for infinite play, or

count of free trial plays.

If the decrypted play count is greater than one, play count) > 0 indicates paid for or free trial plays still remaining

The play count is decrypted by the Party P (C-DSP) using the customer party A's smart card keys, PrK-A, PuK-A, and its vendor secret keys (SeK-V1 .. Vn) and vendor private keys (PrK-V1 .. Vn) and vendor public keys (PuK-V1 .. Vn) and then decremented for accounting purposes, re-encrypted (with an increased customer (family key) sequence number to avoid recorded replay hacker attacks):

```

P-FaK-F(

    vendor identification number (MAC(VIN)),

    session identification number,

    P-PrK-A(P-SeK-Vn(P-PrK-Vn

        (decremented play count,

            vendor sequence number))),

    incremented customer (family key) sequence number,

)

```

and then sent back to the media ticket smart card A for storage.
 If the play count is zero, further media plays or custom
 decryptions are disallowed.

h). the cryptographic digital signal processor (C-DSP) in the
 cryptographic media player, party P, using the:

```

{

    vendor identification number (MAC(VIN)),

    session identification number,
    play code encrypted digital media,

    [(Law Enforcement Access Field (LEAF) for law enforcement
    use only using the embedded movie ticket concept):

        public key courts {public key law enforcement

```

```

{
    appended pass-thru encrypted play code plus
        header,
    vendor private key signed message digest cipher
        (MDC)
}
}

```

identification header from the encrypted digital media,
retrieves the paa-thru encrypted play code with header:

```

{vendor identification number (MAC(VIN)),
    session identification number,
    various layers of encrypted play code with sequence
        number},

```

which may be one of many encrypted play codes even from
different vendors stored in his media ticket smart card A which
is transferred to the cryptographic media player's own tamper
resistant memory. The pass-thru encrypted play code with
sequence number is already digitally signed by the media

distribution vendor's private key, PrK-Vn, and then 3-way encrypted:

Vn-FaK-F(

MAC(VIN),

session id,

Vn-PuK-A(Vn-SeK-Vn

(Vn-PrK-Vn(Vn-SsK-A, vendor sequence number)))

customer (family key) sequence number

) = pass-thru encrypted play code with header.

NOTE:

Sequence Numbers - The sequence numbers are needed to prevent recorded replay attacks on wiretappable buses of pass-thru encrypted signals inside of the cryptographic media player. The vendor sequence number can only be incremented by a party with the vendor secret key (SeK-Vn), customer private key (PrK-n), and system family key (FaK-F) who are the party G for any vendor, the party Vn only for his own play codes and play counts, or the cryptographic media player, party P, for any vendor which player has a collection of all vendor secret keys

(SeK-V1 to Vn) and a collection of all vendor privatekeys (PrK-V1 to Vn). Used in key ownership re-assignment operations by the C-DSP. The player can also check the cryptographic media player, party P, digital signature, and can obtain the customer A's private key (PrK-A) and public key (PuK-A) from customer's inserted media ticket smart card A. The customer (family key) sequence number is for media ticket smart card use only for loop-back operations with the C-DSP.

i). The cryptographic digital signal processor (C-DSP) inside of the cryptographic media player, party P, having all authorized system vendor public keys, PuK-Vn, and all authorized system vendor secret keys, SeK-Vn, which are pre-factory installed by the public key generation authority, party G, must retrieve only the unique vendor's Vn's public key, PuK-Vn, and secret key, SeK-Vn, using the vendor identification number from step 1) and step 5).

j). The cryptographic digital signal processor (C-DSP) inside of the cryptographic media player, party P, uses the system family key (FaK-F), for pass-thru decryption, the customer's private key (PrK-A) obtained from the inserted media ticket smart card A, the vendor Vn's unique secret key (SeK-Vn) and vendor private key (PrK-Vn), to decrypt the digitally signed play code with sequence number, and finally the vendor Vn's unique public key (PuK-Vn) to digitally descramble the play code to give the fully unencrypted play code or session key (1-time secret key) with vendor sequence number:

P-SeK-Vn(P-PrK-A

remove MAC(VIN),

remove session identification number,

remove customer (family key) sequence number,

(P-FaK-F

(pass-thru encrypted play code with header)

)) = temp-j

= still custom encrypted vendor digitally signed play

code with vendor sequence number.

Use of the customer A private key upon the digitally signed
play code will allow play code access:

P-PrK-A(temp-j) = temp-k

= vendor secret key encrypted and vendor digitally signed

(play code, vendor sequence number).

P-SeK-Vn(temp-k) = temp-l

= vendor digitally signed (play code, vendor sequence

number),

$P-PuK-Vn(temp-1) = temp-m = (play\ code,\ vendor\ sequence$
 $number),$

NOTE: Sequence Numbers - (see previous NOTE).

k). The party A's cryptographic digital signal processor (C-DSP), party P, uses the unencrypted play code or session key (D-SsK-A), to decrypt the session key (1-time secret key) encrypted digital medium from party Vn.

l). The party A's cryptographic digital signal processor (C-DSP) will artificially digitally degrade video and audio signals before analog output. This effect will help counter digital recorders wiretapping of 1st generation analog output for further digital to digital music and movie piracy criminal intentions.

A fully digital movie projector using micro-mirror machine (MMM) modules can input encrypted media directly if it has its own decryption digital signal processor function without wiretapping points.

Fully digital loudspeakers can work in a likewise manner with encrypted media.

C). Output by Customer A.

Customers - Party A with Lost, Stolen, Legally

Disputed Smart Cards

The customers, party n, such as party A, party B, etc. (party D, E, F, G, P, S already in use)

which has knowledge of customer identifications and vendor identifications and his own access code to a particular media ticket smart card for toggle field entry into a cryptographic media player, but, no knowledge of whole cryptographic keys stored in cryptographic memory!!!!

for use in lost, stolen, or legally disputed ownership media ticket smart cards.

A). Input of Party D:

1). Customer party A contact the central public key distribution authority (C-PuKDA), party D, with his customer name and public customer identification number (MAC(CIN)) to cancel the old media ticket smart card.

B). Processing by Party D:

1). Party D will mark the old media ticket smart card as cancelled in his database.

```

{

    authorized media distribution vendor identification number
    (MAC(VIN)),

    {---,

    . customer identification number (MAC(CIN)),

    -----,

    customer's public key (PuK-n),

    . eventual registered customer name (retail store
    registered,

    Web registered, or registration postcard),

    lost/stolen/disputed legal ownership field,

    },

}

```

2). Party D will use the public customer identification number (MAC(CIN)) to contact the central public key escrow authorities,

parties E_n , to obtain the split customer private keys from their databases which are indexed by this number, since, the parties E_n have absolutely no knowledge of customer identities.

3). Party D will use the public customer identification number ($MAC(CIN)$) to contact the media distribution vendors, parties V_n , to obtain all the issued encrypted play codes (session keys or 1-time secret keys) with header and sequence number and encrypted play counts with header and sequence number used by customer A. The encrypted play counts may not be up to date or matching of the encrypted play counts in the lost or stolen media ticket smart card, but, if infinite plays are allowed this is acceptable.

The parties V_n have the database records:

```
{  
  
    vendor index number (VIN),  
  
    vendor identification number ( $MAC(VIN)$ ),  
  
    {  
  
        customer identification party A such as name, address,  
        etc.},  
  
        ---,  
  
        customer identification number ( $MAC(CIN)$ ),  
  
        public key of customer A (PuK-A),
```

```

{

    date/time,

    download date,

    download month,

    download year,

    download time,

    title of digital media downloaded,

    session id number,

    paid for amount,

    pass-thru encrypted play code with header &

        vendor sequence number, customer sequence no.

    pass-thru encrypted play count with header &

        vendor sequence number, customer sequence no.

},

```

```

{

    date/time,

    download date,

    download month,

    download year,

    download time,

```



```

        title of digital media downloaded,

        session id number,

        paid for amount,

        pass-thru encrypted play code with header &

            vendor sequence number, customer sequence no.

        pass-thru encrypted play count with header &

            vendor sequence number, customer sequence no.

    },

    etc.

}

```

4). Party D will issue a new media ticket smart card with the previous customer A, private key A, PrK-A, and matching public key A, PuK-A, with the previously issued play codes and play counts. The new smart card will work with existing custom encrypted physical media.

For use in legal transfer of entire ownership of a media ticket smart card A and all custom cryptographic media associated with it from party A to party B. This is called legal "first use."

This is accomplished by use of a cryptographic media player [REF 508] to read from customer party A's media ticket smart card the tamper resistant memory the encrypted 3-way encrypted and digitally signed play code or session key (SsK) with header:

```

Vn-FaK-F(

    MAC(VIN),

```

session identification,

$Vn-PuK-A(Vn-SeK-Vn($

$Vn-PrK-Vn(Vn-SsK-A, \text{ vendor sequence number}))$

customer (family key) sequence number

) = 3-way encrypted and digitally signed, pass-thru

encrypted play code with header (and sequence numbers).

NOTE: Sequence Numbers - (see previous NOTE on sequence no's).

Where:

Vn = the media distribution party

F = family key or group secret key

$A-PuK-B$ = party A using the public key for party B

The cryptographic media player [REF 508], party P, can partially decrypt party A's play codes or session key ($SsK-A$) in his media ticket smart card A, and re-encrypt it over to party B's play codes or session key ($SsK-B$), by the decryption steps:

$P-FaK-F(\text{encrypted play code with header (and sequence numbers)})=$

{vendor identification number ($MAC(VIN)$),

session identification number,

customer A public key encrypted,

vendor secret key encrypted,

vendor digitally signed {play code,

vendor sequence number + 1},

customer (family key) sequence number + 1} = temp-B1.

Remove MAC(VIN), remove session identification number, and
customer (family key) sequence number from temp-B1 = temp-B2.

Apply customer A private key to temp-B2 to decrypt it to temp-B3.

Apply vendor secret key to temp-B3 to decrypt it to temp-B4.

Apply vendor public key to temp-B4 to de-scramble it to temp-B5.

Increment vendor sequence number in temp-B5.

Party P (C-DSP) then does the key ownership change re-encryption
steps for customer B:

P-FaK-F(vendor identification number,

Session identification number,

P-PuK-B(P-SeK-Vn(

P-PrK-Vn(temp-B5),

customer (family key) sequence number + 1

) = temp-B6,

which changes the public key encryption of customer A to the public
key encryption of customer B. The public key of customer B, PuK-B,
must be obtained from some internet connected source as public
information. The re-encrypted play code with header, Z, can be
returned to the media ticket smart card of party B.

C). Output by Party D:

None.

Federated Cryptographic Architecture

A). Central layer - media ticket smart card system authority, party S, which has the entirely separated and autonomous functions of:

central public key generation authority (104), party G,

central public key distribution authority (108), party D,

central public key escrow authorities (TBD), parties En,

using an embodiment of the media ticket smart card public key cryptography algorithm, central public key distribution authority database ID number 0 (112), and central public key distribution authority key escrow agents (128) for optionally holding split private keys and family keys. This layer does pre-factory preparation of media ticket smart cards.

B). Local layer - authorized media distribution companies, Vn, which own the digital media.

C). Customer layer - customer parties A, B, C, G, etc. using any prior art customer residence or customer business personal computers (200) and the use of media ticket smart cards (212) A-n, matched to each customer such as media ticket smart card A matched to customer A, media ticket smart card B matched to customer B, etc. which are used to hold cryptographic customer private keys and encrypted play

codes (session keys or 1-time secret keys) with header and encrypted play counts (paid for numbers of plays, -1 for infinite plays, or counts of free trial plays) with header.

Fig. 2 is a circuit block diagram of a prior art cryptographic microprocessor unit with tamper resistant non-volatile electrically erasable programmable read only memory (TNV-EEPROM) found in a prior art smart card.

Fig. 3 is a circuit block diagram of a prior art media ticket smart card (212) containing a cryptographic microprocessor. This is used for secret key and private key secure containment and physical transportation.

Fig. 4 is a circuit block diagram of a prior art media ticket smart card reader attached to a personal computer.

Media ticket smart card reader

This cryptographic device consists of:

A). A built-in or embedded, crypto-microprocessor integrated circuit (C-uP) (see above) used for pass-thru encryption.

B). A physical contact or optical (non-physical contact) connector to a smart card.

A physical contact can provide a power pin which makes a watch battery unnecessary on the Smart Card.

C). I/O circuitry is a universal serial bus (USB) bus connection to an external personal computer.

D). Durable packaging which is weather resistant, electrostatic resistant, electromagnetic resistant, temperature extreme resistant, grease resistant, etc.

E). Package is credit card reader sized, but, slightly thicker and slightly heavier.

F). External to device printed labeling:

customer's name

customer's address

customer's identification

authorization sticker of trusted smart

card reader licensing and expiration date.

The media ticket smart card readers have no secret construction and can be publicly reviewed and commercially manufactured.

Fig. 5 is a circuit block diagram of a crypto digital signal processor chip (C-DSP) (932), future patent pending [REF 500]. This is used for doing hybrid key cryptography which is both public key cryptography and fast hardware based secret key cryptography with hardware block error detection and correction all done inside of a digital signal processor with Moving Picture Expert's Group (MPEG-X) decompression support.

Crypto Digital Signal Processors (C-DSP's)

See [REF 500], future patent pending.

NOTE: This is a new type of full custom integrated circuit (IC) in a single-IC package (having no external wiretapping points) consisting of:

A). a 32-bit or 64-bit cryptographic digital signal processor (DSP) used instead of dedicated circuitry for flexible updates with new algorithms and handling longer secret and private keys. Used for analog to digital signal (ADC) conversion, digital processing of analog signals, and digital to analog signal conversion (DAC). Firmware support for hybrid key cryptography for use with a separate hardware secret key decryption only circuit (e.g. 56-bit Data Encryption Standard (DES) in triple key mode and also several cipher block chaining modes and stream cipher modes) which also does hardware block error detection and error correction critical with block chaining cipher modes. Firmware support for coordinated use with a separate MPEG X decompression only circuit for most commercial play-only applications for music, movies.

B). Tamper resistant, non-volatile, electrically erasable programmable read only memory (TNV-EEPROM) for crypto key storage

of private keys, secret keys, session keys, family keys, and often used public keys, and crypto algorithm and protocols program store,

C). Static random access memory (SRAM) for temporary data store,

D). I/O circuitry:

direct memory access (DMA) controllers,

memory address strobing,

programmable interrupt controller (PIC)

E). counter timer circuits (CTC's)

F). A true random number generator -

e.g. a radioactive source or electronic random noise emitter

G). A hardware circuit to do large integer to large integer exponentiation with a modulo (remainder) function by the "binary square and add method" which will be used for fast public key RSA (R), DSA (R), Diffie-Hellman (R) encryption of the RSA form:

$$\text{Cipher Text} = (\text{Plain Text}) \exp (e) \text{ modulo } n$$

where e is the encryption public key integer, and

n is a large prime integer number base.

and decryption of the RSA form:

$$\text{Plain Text} = (\text{Cipher Text}) \exp (d) \text{ modulo } n$$

where d is the decryption private key ~~private-key~~ integer, and n is the same.

H). A hardware circuit to do fast session key 1-time secret key (SsK-n)) "on the fly (up to 16 megabytes/sec)" secret key decryption of the digital signal retrieved from physical medium (e.g. hard disk, EEPROM memory card, DVD-RW, DVD+RW, CD-R).

This can be an existing IBM patented Data Encryption Standard (DES) integrated circuit used in a silicon compiler library as a added function in a larger chip.

Standard secret key algorithm is 56-bit standard Data Encryption Standard (DES R)) in triple key mode, cipher block chaining (CBC) mode, electronic codebook (ECB) mode, cipher feed-back mode (CFB) mode, and output feedback mode (OFB) mode.

Standard DES substitution (S)-boxes and permutation (P)-boxes are used and are firmware downloadable with the entry of special hardware access keys.

Built-in hardware block error detection and error correction circuits necessary to prevent rampant error propagation when using block chaining modes.

NOTE: Linear feedback shift register (LFSR) circuits are easily cracked by hackers and should be avoided!!!!

I). A cryptographic hardware circuit to do fast digital signal processing (crypto-DSP) of the already hardware decrypted but still MPEG-X compressed digital audio/video signal. The "cipher text" or session key encrypted MPEG-X compressed digital signal was - retrieved earlier from physical storage medium (e.g. hard disk,

EEPROM bank programmable memory card, digital versatile disk (DVD), compact disk (CD)).

In this patent's application area, the MPEG-X compressed digital data is entirely one way read from physical recording medium, put through block error and detection circuitry (which may be combined with the decryption circuitry), session key DES (R) decrypted with the play code, MPEG-X decompressed, digitally artificially degraded (an option for analog watermarking of some form is possible), converted to analog and played. There is no need for the reverse unencrypted and uncompressed "plain text" medium to compressed and encrypted "cipher text" medium process as in general 2-way cryptography messaging. See BACKGROUND - Cross-References To My Related Inventions - A Cryptographic Digital Signal Processor, patent pending [REF 500].

The future patent pending crypto-DSP's [REF 500] will be custom, single chip integrated circuit (IC) to avoid external and internal wiretapping points. A wire-mesh intermetallic layer on the top of the chip with load impedance monitoring circuits is used to detect test probes which will initiate erasure of the TNV-EEPROM crypto memory. The chip will use a cryptographic digital signal processor (crypto-DSP) to coordinate hardware error detection and correction, fast hardware session key (SsK-n) DES (R) decryption, MPEG X hardware digital decompression, and then "playing" of the session key (SsK-n), custom encrypted, MPEG X compressed, digital media retrieved from physical medium. They will artificially digitally

degrade signals before analog output to counter digital recorder piracy of wiretapped 1st generation analog signals.

The alternate technology to counter 1st generation analog signal theft is to add analog watermarks. Analog watermarks come in two forms. The first form is pseudo-random fine-line background noise imperceptible to the human eye or ear which can be used to audit trail source and copyright status of digital media meant to counter digital recordings of 1st generation analog output. The second analog watermark form is used in video data for human perceptible, subtle, pseudo-random, edge pattern effects which do not disturb the viewer, but, can be measured for audit trail purposes and is meant to counter "premier movie" digital video-camera tape recordings. In y. 2002, analog watermarks are not proven as to being hacker proof given the hacker use of powerful personal computer digital signal processing filter programs. The analog output will go to analog loudspeakers. Digital output modulated to analog will go to computer digital video displays (e.g. SVGA, UXGA computer monitors).

The crypto-DSP's for an audio only cryptographic media player (e.g. cryptographic MP3 player) future patent pending [REF 508] will be a custom integrated circuit (IC) combined with silicon compiler circuitry in a single integrated circuit with built-in functions of:

digital signal processing (crypto-DSP) functions and also

coordination and byte shuffling,

fast hardware block error detection and correction,

fast hardware session key (1-time secret key) or session key (SsK-n) DES (R) decryption unit using IBM's patented Data Encryption Standard (DES),

fast hardware MPEG X decompression,

tamper resistant non-volatile electrically erasable programmable read only memory (TNV-EEPROM) for crypto keys and crypto computer programs

a hardware true random number generator such as a random noise circuit

a hardware circuit to do large integer to large integer exponentiation with a modulo (remainder) function by the "binary square and add method" which will be used for fast public key RSA (R), DSA (R), Diffie-Hellman (R) encryption and decryption of the form:

$$\text{cipher text} = \text{plain text}^{\text{exponent}} \pmod{n}$$

where e is the encryption public key integer,

and n is a large prime integer number.

n-channel digital audio signal processing as from digitally compressed MPEG X audio retrieved from physical medium.

n-channel MPEG X audio "one-half codec" (only MPEG X decompression for n-channels is needed with no MPEG X compression functions)

n-channel artificial digital audio signal degradation,

n-channel digital to analog signal converters with line amplifiers for output to analog loud-speakers,

The crypto-DSP's for an audio/video cryptographic media player patent pending [REF 508] will be a custom integrated circuit (IC) with built-in functions of:

digital signal processing (crypto-DSP) functions

and also coordination and byte shuffling,

fast hardware block error detection and correction,

fast hardware session key (1-time secret key) or session key (SsK-n) DES (R)decryption unit using IBM's patented Data Encryption Standard (DES),

fast hardware MPEG X decompression,

tamper resistant non-volatile electrically erasable programmable read only memory (TNV-EEPROM) - for crypto keys and crypto programs

a hardware true random number generator such as a random noise circuit

a hardware circuit to do large integer to large integer exponentiation with a modulo (remainder) function by the "binary square and add method" which will be used for fast public key RSA (R), DSA (R), Diffie-Hellman (R) encryption and decryption of the form:

$$\text{cipher text} = \text{plain text}^{\text{exponent}} \pmod{n}$$

where e is the encryption public key integer,

and n is a large prime integer number.

digital video signal processing

n-channel MPEG X audio/video "one-half codec" (only n-channel MPEG X audio (2-channel)/video decompression is needed with no MPEG X compression)

artificial audio/digital video signal degradation,

digital to analog video signal converters such as a random access memory digital to analog converters (RAMDAC) and line amplifiers.

digital to digital video signal converters and line amplifiers such as a random access memory digital to analog converter (RAMDAC) (e.g. digital modulated to analog output of SVGA RAMDAC, UXGA RAM-DAC).

n-channel digital to analog signal converters with line amplifiers for output to analog loud-speakers,

The crypto-DSP's for a video only electronic book or electronic newspaper cryptographic media player **future** patent pending [REF 508] will be a custom integrated circuit (IC) combined in a single integrated circuit with built-in functions of:

digital signal processing (crypto-DSP) functions and also coordination and byte shuffling,

fast Reed-Solomon (RS) hardware block error detection and correction preferably included with the hardware secret key decryption hardware,

fast hardware session key (1-time secret key) or session key (SsK-n) DES (R) decryption only unit for 'canned media' players using IBM's patented Data Encryption Standard (DES),

fast hardware MPEG X decompression,

tamper resistant non-volatile electrically erasable programmable read only memory (TNV-EEPROM) - for crypto keys and crypto programs

digital video signal processing n-channel MPEG X video only "one-half CODEC" (only n-channel MPEG X audio (2-channel)/video decompression is needed with no MPEG X compression)

artificial audio/digital video signal degradation,

digital to analog video signal converters such as a random access memory digital to analog converters (RAMDAC) and line amplifiers.

digital to digital video signal converters and line amplifiers such as a random access memory digital to analog converter (e.g. digital modulated to analog output of SVGA RAMDAC, UXGA RAMDAC).

The cryptographic DSP's have no secret construction and can be publicly reviewed and commercially manufactured.

HACKER ATTACKS UPON THE

CRYPTO-DSP

A hacker party wishing to get a digital sound or video master copy for illegal distribution merely has to tap off with alligator clips the wires going to the analog speakers for a 1st generation analog digital copy (which will experience no further degradation in digital to digital copying). The resulting digital signal will be a copy of a clear-text, 1st generation analog signal which is countered by an artificially digitally degraded signal. Video wiretapping of 1st generation analog video signals is more difficult because the digital modulated to analog output (analog R'G'B') which goes to a coputer monitor like digital television screen is very high frequency. A sampling digital mode at the screen refresh rate might capture an acceptable digital pirated copy. The pirate can simply use a digital videocamera to videotape a movie screening in 1-channel sound while adding the wiretapped audio track later on. Another counter to 1st generation analog copying is analog watermarking as explained in the crypto-digital signal processor (C-DSP) section just above. The analog watermarkings are currently in y. 2002 not technically proven as being safe from hacker personal computer filtering. The recording into a digital recorder will give the hacker a very high quality clear-text, digital master of a 1st generation analog signal for illegal distribution and unlimited and perfect digital to digital reproduction without further signal degradation unlike old analog to analog or analog to digital copy

methods. A few digital copies for personal customer use are allowed as "fair use" under the US Copyright laws.

A clear-text digital audio master can be run through a Motion Pictures Electronics Group, Standards Version I Audio Compression Layer 3 (MPEG I audio layer 3 or shortened to MP3) computer program. The resulting MP3 file (even of internationally copyrighted material) can be freely distributed on the internet over peer-to-peer, Web file sharing services such as Napster (R) brand, Gnutella (R) brand. The illegal distribution for profit of copyrighted material is a US Federal felony. The illegal distribution for non-personal use copies of copyrighted material is a US misdemeanor. Such services are widely used in the year 2001 for illegally distributing music from compact disks (CD's). CD audio was never encrypted giving hackers access to the audio, digital master.

A clear-text audio/video master can be obtained by similar illegal recording techniques. Digital video movies can be distributed in the same illegal manner. The Content Scrambling System (CSS) (R) is a standard 1990's "on the fly" digital encryption scheme used by digital versatile disks (DVD's) for storing movies. The technology is based upon a pair of linear feed-back shift registers (LFSR) which is an old technology easily cracked by personal computer (PC) simulation programs in the year 2001. A hacker attack by a Swedish group called "Anathema" in the year 2001, cracked this code giving hackers access to the digital masters of DVD distributed movies and movie soundtracks.

Fig. 6 is a circuit block diagram of a cryptographic media player, **future** patent pending [REF 508] with a built-in media ticket smart card reader.

Internal (to PC) Cryptographic

Media Players (patent pending) [REF 508]

These are peripheral component interconnect (PCI) I/O computer bus crypto-sound cards and PCI bus crypto-video and AGP bus crypto-video cards. Each card is based upon an embedded crypto-DSP.

External (to PC) Cryptographic

Media Players (patent pending) [REF 508]

These are future versions of today's MP3 players which play digital audio in compressed MP3 digital format. Future stand alone versions will have controlled digital media in custom encrypted form. These will be called crypto-MP3 players, crypto-CD players, and crypto-DVD players. These are all based around an embedded crypto-DSP.

An interesting example of this class will be a stand-alone smart appliance which will be internet connectable, have a media ticket smart card reader interface, have a crypto toggle data entry field or future bio-identification reader such as a digital fingerprint reader, have an embedded crypto-DSP core, have cryptographic media or 1-way transfer of custom session key encrypted media writing capabilities, crypto media reading capabilities, and a crypto-DSP for media playing. This type of transition device will allow secure recording of crypto media during the period of industry transition from non-crypto CPU based PC's to crypto-CPU based PC's.

The above internet connected example only with cryptographic writing capabilities for different user selected types of media (e.g. DVD-RW, CD-RW, CD-R, FLASH (R) Memory Card, can provide a store juke-box machine for dispensing crypto media for users without a crypto-PC, but, with external or internal cryptographic media players [REF 508].

ADVANTAGES - Over the Prior Art -

Preferred Embodiment

A. An advantage of this invention is to support physical distribution of internet "downloaded" custom encrypted digital media (see REFERENCES - NON-PATENT LITERATURE [REF 500] - "The Secure Digital Music Initiative (SDMI)") which is "played" or decrypted upon a special cryptographic media player with inserted portable media. The portable media may also be purchased directly from the retail store.

One implementation for digital media distribution is to use custom encryption of digital media factory or internet deposited onto compact disk record once (CD-R), digital versatile disk read/write (DVD-RW (R), DVD+RW (R)), or flash memory cards (FLASH). Matching removable and easily transportable prior art media ticket smart cards will provide custom encryption and decryption by securely containing cryptographic keys called customer private keys, PrK-n, encrypted play codes (session keys or 1-time secret keys) with headers and also encrypted play counts (paid for numbers of play, -1 for infinite plays, of counts of free trial plays) with headers. The media ticket smart cards can be remotely programmed over the internet using prior art media ticket smart card readers attached to prior art personal computers.

The encrypted digital media is either factory distributed in physical form or else remotely internet downloaded. The matching media

ticket smart card is also either factory distributed or internet updated. Only encrypted ("red") media with unlimited copy potential is allowed upon any wiretappable ("red") or public cables and buses, computer disks, CD's, DVD's, FLASH (R) Memory Cards (EEPROM). The custom encrypted digital media and the matching media ticket smart card must be physically transferred and attached to a cryptographic media player [REF 508].

At the cryptographic media player [REF 508], the media ticket smart card must be inserted into a media ticket smart card reader in order to deposit the encrypted play code with header and encrypted play count with header over wiretappable ("red") computer buses into the smart media player's crypto-digital signal processor unit [REF 500]. The physical medium must be inserted into the smart media player. Thereafter, the cryptographic digital signal processor unit [REF 500], can do custom decryption of custom encrypted digital masters done "on the fly." A crypto-audio player will just have a crypto-audio unit based upon a crypto-digital signal processor [REF 500]. A crypto-video player will be a computer with a crypto-video card (252) and crypto-sound card (252). Outputted decrypted analog sound and video ("red") must be digitally degraded before digital to analog conversion (DAC) to avoid giving away digital masters. The alternate technology of analog watermarking of analog output to counter signal piracy in y. 2002 is mathematically unproven as hackers can easily run computer filter programs to eliminate such extraneous signals.

The effective use of custom encrypted computer programs, multi-media programs, and computer games is left out of this patent for a

number of reasons. The main difficulty here is that digital computer code is involved along with digital computer data. The digital computer code because it hops around in program counter execution cannot be decrypted real-time unlike the computer digital data which is accessed sequentially. A new type of crypto-personal computer (C-PC) with a new type of cryptographic operating system (C-OS) containing a new type of crypto-central processing unit (C-CPU) must be developed which runs off of a "disk vault" or secure ("black") area of the computer hard disk holding already decrypted computer programs for CPU execution speed and either decrypted computer data needing real-time decryption or undecrypted computer data. This secure hard disk area called a "disk vault" is classified erased upon computer power-down. A non-secure ("red") area of the computer hard disk holds encrypted data or else non-classified data. A "disk vault" or encrypted hard disk mountable disk volume may also be used which holds classified data files and classified computer programs which are encrypted upon power-down or no keyboard use for a programmed period and decrypted upon computer power-up and disk mounting.

This patent limits itself to giving structure and a cryptographic architecture to a new type of cryptographic media player [REF 508] which contains a cryptographic digital signal processing chip [REF 500] and a built-in media ticket smart card reader.

This patent also gives a cryptographic structure to secure pass-thru encryption mechanisms for moving internet downloaded crypto keys over wiretappable ("red") prior art computer buses existing on prior art personal computers.

B. An advantage of this invention is to use only one media ticket smart card per owner with many digital media distribution vendors.

This is accomplished by having factory pre-installed public key cryptography matched pairs of private keys and public keys with a private key for customer A held in his own media ticket smart card and the matching public key for customer A publicly available on the internet. Also family keys or common secret keys are factory pre-distributed to relevant and authorized system users and components.

This is accomplished by having different media distribution vendors (e.g. Disney/ABC Capital Cities, AOL/Time-Warner, EMI Music, Arista Records, Polygram Records, Bartlesmann, etc.) internet world wide web download session key (1-time secret key) encrypted digital media to disk and its matching pass-thru encrypted play code and encrypted play count downloaded to party A's media ticket smart card.

C. An advantage of this invention is to allow the owner's one media ticket smart card to be used with any owner's cryptographic media player [REF 508].

This is accomplished by having common media ticket smart cards and media ticket smart card readers in every cryptographic media player [REF 508] with standards based media ticket smart card public key cryptography protocols.

D. An advantage of this invention is to stop the use of any unauthorized digital copying of digital media.

This is accomplished by the use of custom session key (1-time secret key) encryption of digital media. This media is useless without the customer's media ticket smart card programmed with a matching encrypted play code (pass-thru encrypted session key or 1-time secret key) with header and encrypted play count (paid for number of plays, -1 for infinite plays, or number of free trial plays) greater than 0 with header.

E. An advantage of this invention is to restrict one digital media distribution company's unencrypted digital masters only to itself and absolutely no other party especially access by any other competing digital media distribution company.

This is accomplished by the media ticket smart card system authority being broken up into three entirely separate functions and groups:

the public key generating authority, party G, (access to private keys and family keys but no access to customer identifications)

the public key distribution authority, party D (access to customer identifications but no access to private keys or family keys),

the public key escrow authorities, party E1 and party E2 (E1 has access to only half of key split private keys, and half of key split family keys, but, no access to customer identifications).

In addition, use of the media distribution company (Vn), unique secret key (SeK-Vn), known only by the public key media ticket smart card system authority, the optional key escrow parties (party K1 and party K2), the owning media distribution company (party Vn), and the cryptographic media player [REF 508] having a copy of all such secret keys for all vendors in its secure memory.

F. An advantage of this invention is to allow play counts or count controlled plays or counted decryptions of custom encrypted media including counts of free trial media plays.

This is accomplished by the use of custom session key (1-time secret key) encryption of digital media. This media is useless without the customer's media ticket smart card programmed with a matching encrypted play code (pass-thru encrypted session key or 1-time secret key) with header and encrypted play count (paid for number of plays or number of free trial plays) greater than 0 with header.

G. An advantage of this invention is to provide all public key cryptography legal attributes such as:

- 1). authentication (like an exchange of photo ID's or thumbprints)
- 2). encryption/decryption (for privacy)
- 3). integrity (wholeness or non-tampering)
- 4). digital signatures (like handwritten signatures)
- 5). non-repudiation (denying digital signatures)
- 6). authorization (approval using digital signatures and dating or official post marks)
- 7). archiving (storing digitally signed documents in a high integrity environment)
- 8). accessibility (restricting access to authorized users)
- 9). audit trail (recording accesses to information with public key ID's, dates, times, and locations)
- 10). play counts/play codes for counting paid for and authorized personally encrypted digital media plays and for decrypting them
- 11). crypto key splitting and key escrow.

12). crypto key administration and key architectures.

The invention provides these legal attributes through the use of hybrid key cryptography which is public key cryptography combined with secret key cryptography, smart cards, and key escrow concepts. Public key cryptography provides authentication, secret key exchanges, integrity using private key signed message authentication ciphers (MAC's) and message digest ciphers (MDC's), digital signatures using private key signed MDC's, authorization using digital signatures.

Secret key cryptography provides fast software and hardware based encryption/decryption.

Smart cards provide non-repudiation using crypto memory for all crypto keys, audit trail, accessibility, and archiving using registered smart cards, and play codes and play counts stored in smart card crypto memory.

Key escrow cryptography provides crypto key splitting and key escrow architectures.

H. An advantage of this invention is to support pass-thru encryption of play codes (session keys or 1-time secret keys) and play counts (paid for numbers of plays, -1 for indefinite plays, or counts of free trial plays) for their trip from a media distribution company's central web server over the open internet to a customer's personal computer over wiretappable buses to a secure, cryptographic memory inside of a smart card inserted into a media ticket smart card reader attached to the personal computer.

I. An advantage of this invention is to support physical transfer of encrypted digital media in the form of digital versatile disk read/write (DVD-RW (R), DVD+RW (R)), compact disk record once (CD-R), and bank programmable solid state memory cards (FLASH (R)), and also the physical transfer of media ticket smart cards from a customer's personal computer (PC) to a cryptographic media player [REF 508] (e.g. crypto-MP3).

J. An advantage of this invention is to support pass-thru encryption of cryptographic keys in the form of play codes (session keys or 1-time secret keys) and play counts (paid for numbers of plays, -1 for indefinite plays, or counts of free trial plays) from a smart card inserted into a media ticket smart card reader built-into a cryptographic media player [REF 508] for transferring such keys over wiretappable ("red") computer buses to a cryptographic digital signal processor unit having its own tamper resistant non-volatile electrically erasable programmable read only memory which processor is contained inside of the cryptographic media player [REF 508].

Examples are pass-thru, encrypted, transfer of keys from smart cards to media ticket smart card readers (using media ticket smart card reader vendor family keys) to crypto-DSP's (using crypto-DSP vendor family keys) to crypto-CPU's (using crypto-CPU vendor family keys) to crypto-OS's (using crypto-OS family keys) to crypto-software (using crypto-software family keys).

K. An advantage of this invention is to support an optional citizen/customer media ticket smart card authentication triangle between the three points of:

point 1, customer A to (a first means of a passphrase/passcode, a second means of a bio-identification such as a digital fingerprint, a third means of a password mixed with pseudo-random noise called salt), to

point 2, media ticket smart card A holding customer A's private keys, secret keys, session keys, encrypted play codes with header, and encrypted play counts with header to prevent the use of stolen media ticket smart cards, to

point 3, cryptographic media player [REF 508].

Any one of the three points which are detected as unauthorized will stop the media ticket smart card read/write process. An authorized cryptographic media player should have a certified sticker for the customer to inspect.

The passphrase/passcode (passcodes are the shorter form but hard to remember) will be customer input into a toggle field with liquid crystal display (LCD) placed in the cryptographic media player. The cryptographic media player may also have a built-in fingerprint

reader. The cryptographic media player will have a built-in media ticket smart card reader.

The cryptographic media player will match the customer input passphrase/passcode with the one "burned in" the inserted media ticket smart card. A mismatch will give a customer warning on the LCD display and a "beep." Alternately, a customer fingerprint can be matched with one "burned in" the media ticket smart card. No fingerprint records are kept.

L. An advantage of this invention is to support a cryptographic media authentication triangle between the three points of:

point 1, a copy of 1-way transfer of custom session key encrypted digital media A, to

point 2, media ticket smart card holding customer A, or user's private keys, secret keys, encrypted session keys (play codes), encrypted play codes with header, and encrypted play counts with header (play counts), to

point 3, cryptographic media player [REF 508].

Any one of the three points which are detected as unauthorized will stop the custom encrypted digital media playing process.

The cryptographic media player will match the inserted custom encrypted media with the play code from the inserted media ticket

smart card. A test strip of media will be decrypted of known values to confirm a match. A mismatch will warn the customer upon the LCD display and a "beep."

M. An advantage of this invention is to support legal "fair use" of US copyrighted encrypted digital media or the archiving of two to three copies for personal use. The purpose of "fair use" is to allow for recovery in case of accidental damage, theft, fire, flood, natural disaster, legal archiving, disputed legal ownership (as any divorced person will recognise), or one or at most two convenience copies in multiple locations used by the legal owner. Legal "fair use" also supports a home set of media and an auto set of media.

This is accomplished by customer session key (1-time secret key) encrypted media which can be copied any number of times for archiving. Any custom encrypted copy must be decrypted by the matching media ticket smart card.

Non-copyrighted commercial and home-made material is kept in unencrypted form and can be copied an unlimited number of times and played an unlimited number of times.

Two encrypted copies can be made for a home media set and a car media set all under legal "fair use." Two sets of matching media

ticket smart cards will allow legal use by the customer at his home and his car.

A primary and back-up pair of media ticket smart cards for customer A can be inserted into a crypto-digital signal processing chip in a crypto-media player to do a card update operation to make the two cards' play codes and play counts match exactly. This operation is done by first inserting one media ticket smart card and then another into the crypto-media player with crypto operations similar to "first use" just below done on each card with 2-way commit operations done in multiple loop-backs before finalizing operations per card.

N. An advantage of this invention is to support legal "first use" of US copyrighted encrypted digital media or the right of one person to sell or transfer in entirety the encrypted digital media to another person and transfer only relevant media ticket smart card cryptographic keys to the other person's media ticket smart card.

This is accomplished by use of a cryptographic media player [REF 508] to read from customer party A's media ticket smart card the tamper resistant memory held encrypted play code (session key (SsK) or 1-time secret key):

Vn-FaK-F(MAC(VIN),

session id,

{Vn-PuK-A(Vn-SeK-Vn(

vendor digitally signed {play code with sequence number})),

),

customer (family key) sequence number,

) = temp-N

= pass-thru encrypted play code with header (and sequence no's),

NOTE: see previous NOTE on sequence numbers.

where V_n = the media distribution party,

F = family key or group secret key

$A\text{-PuK-B}$ = party A using the public key for party B

The cryptographic media player [REF 508] party P can fully decrypt, update the vendor sequence number, and then re-encrypt party A's play codes in his media ticket smart card A, over to party B's play codes by the decryption steps:

$P\text{-PuK-}V_n(P\text{-SeK-}V_n(P\text{-PrK-A}(\text{remove MAC(VIN)},$

remove session id,

remove customer (family key) sequence number,

$P\text{-FaK-F}(\text{temp-N})) = \text{temp-N1},$

Party P increments the temp-N1 vendor sequence number = temp-N2,

and then the re-encryption steps:

$P\text{-FaK-F}(\text{MAC(VIN)},$

session id,

$P\text{-PuK-A}(P\text{-SeK-}V_n($

$P\text{-PrK-}V_n(\text{temp-N2}))),$

customer (family key) sequence number + 1) = temp-N3,

which changes the private key encryption of customer A to the private key encryption of customer B. The re-encrypted play code with header and sequence number, Z, can be returned to the media ticket smart card of party B.

O. An advantage of this invention is to support lost and stolen media ticket smart cards.

Customers will probably be allowed by most vendors to have two media ticket smart cards both programmed with the same play codes and play counts. This will allow legal use of encrypted media in two places such as a home and a vehicle. If one media ticket smart card is lost or stolen, the customer's encrypted media collection which may be worth several thousand dollars is still accessible with the other spare media ticket smart card. The customer may then apply for a media ticket smart card duplication process over the Web.

If a customer loses both matching media ticket smart cards programmed for him or one of a single issued media ticket smart card, or a legal ownership dispute is decided by a court, a recovery process is possible. A completely lost media ticket smart card (holding encrypted play codes with header and encrypted play counts with header) of purchased music or movies can be reported in to the media ticket smart card system authorities who will de-activate the lost media ticket smart card. They will issue a new media ticket smart card replacement with a new customer public key/private key pair and re-constructed encrypted play codes with header although exact values of former play counts will not be recovered.

A completely stolen media ticket smart card reported as such can be electronically deactivated by the media ticket smart card system authorities who will de-activate the lost media ticket smart card. They will issue a new media ticket smart card replacement with a new customer public key/private key pair and re-construct encrypted play codes although exact values of former play counts will not be recovered.

P. An advantage of this invention is to support non-copyrighted commercial material, home produced material, and previously recorded, non-encrypted digital Copyrighted material by allowing unlimited unencrypted plays of the media.

This is accomplished by a by-pass switch in the cryptographic digital signal processor (C-DSP) within the cryptographic media player which will allow the cryptographic digital signal processor to skip decryption and do regular digital decompression processing in example for previously existing MPEG I Audio Layer 3 (MP3) decompression for MP3 compressed music recordings or MPEG IV movie recordings.

Q. An advantage of this invention is to prevent use of this strong cryptography system of software and hardware by terrorist forces and countries which are enemies of the United States for military use of Command, Control, Communications, Computers, and Coordination (CCCCC or C Five).

This is accomplished for US jurisdiction vendors and US jurisdiction users by licensed encryption and the legally required use of key escrow of cryptographic keys placed into the hands of a minimum of two neutral, licensed escrow second parties along with the legal forcing of a pass-thru encrypted play code with header appended to the encrypted digital data. With law enforcement obtainment of a court order with 4TH AMENDMENT "probable cause" of a crime or a FISA court order for "national security" cases only, Federal, state, or local law enforcement could get from the key escrow parties copies of key split cryptographic keys. Media ticket smart cards will allow use of whole

cryptographic keys in a cryptographically secure container which is a crypto-microprocessor with tamper resistant non-volatile electrically erasable programmable read only memory (TNV-EEPROM) which cannot be illegally copied. All legitimate cryptographic key copies should be transferred from cryptographic hardware to cryptographic hardware or from 'black' hardware to 'black' hardware with use of family key (shared secret key) based pass-thru encryption over all "red" or wiretappable buses and networks.

If suspected criminal activity occurs within US jurisdiction, law enforcement can get a court order for a "cipher text (encrypted)" wiretap or a legal wiretap of encrypted data sent over the Internet which can be stored for later decryption. This "cipher text (encrypted)" wiretap can be decrypted at later dates by law enforcement in case of an actual crime or in case of "probable cause" or FISA court order of a criminal or terrorist action by obtaining appropriate key split cryptographic keys held in key escrow by the licensed US vendor who is a commercial, public key distribution authority (PuKDA). If the central hub is in US jurisdiction, the public key distribution authority (PuKDA) will be a licensed encryption vendor and will be required by proposed US Federal law to use the key escrow provisions. The key excrow keys are used upon the appended pass-thru encrypted play codes with headers to recover the session keys used to decrypt the cipher text media. The standard commercial media intended by this patent being hub centered in Hollywood, California using worldwide downloaded commercial, digital music, commercial, digital movies, and commercial,

digital entertainment sold by legitimate and well known media distribution companies. The media content cannot be restricted by technology alone. A rogue nation may send any digital media using the software and hardware. The media ticket smart card digital media data under the proposed patented cryptographic protocols is useful for military use because it can also only be sent openly over the internet in strong cryptography form only one-way, from hub to spoke and not from spoke to hub, used to dynamically distribute session keys for two-way communications.

Hidden back-door cryptography key use also called an uneven or non-linear key space for use with the hardware specified in this invention is not advisable. An open hardware architecture with open 3rd party fabrication and open academic and industry review precludes any use of uneven or non-linear key spaces. Leaks of the hidden key would quickly propagate through hacker Web sites and verbal leaks without strong espionage laws for US Department Of Defense classified material resulting in massive holes in the system.

(PROPOSED LEGISLATION) A Federal law licensing program for use of strong cryptography within US jurisdiction with mandatory key escrow is highly recommended limiting licensed access to trusted commercial parties based upon establishing a legal environment of:

- 1). "legal record keeping" of signed, witnessed, and dated
hardcopy and electronic record keeping using digital signatures,
digital US Post-marked dates,

2). "legal complaint filing"

3). a "due process" type of internal legal review,

and "duely diligent" actions in resolving illegal issues

including contacting outside law enforcement and filing charges
for judicial action.

which legal environment includes compliance with 1). all Federal and
individual US state laws, 2). local municipal laws and city ordinances,
and 3). a lack of criminal history among management personnel.

(PROPOSED LEGISLATION) Federal jurisdiction established along
"virtual US borders" at the Federal, state, and local levels will allow
"electronic policing" of all cryptography from terrorist groups and
enemy nations coming into the United States over the global Internet.
Bandwidth bottlenecks can be avoided by optical hardware and special
cryptography tools. This "electronic virtual filtering" will be done
in order to enforce the proposed US legal requirement of licensed
encryption from licensed and trusted vendors of all cryptography on US
soil with key escrow provisions. All worldwide Internet traffic will
be controlled with US and foreign smart passport cards, US and foreign
smart driver's license cards, commercial media ticket smart cards,
commercial smart credit cards, etc. The use of smart cards will give
to all internet data the 12 legal attributes mentioned in the earlier
prior art section of this patent necessary for use in US, foreign, and
international courts of law. A proposed global electronic US postal
office is realizable giving electronic US Postal stamp information of

authentication (who) information, location from digital US Postal Stamps (where), routing from global IP addresses (where), US Postal GPS digital GPS time stamps (when), with strong encrypted letter contents under digital integrity checks (what - like digital ink watermarks), and digital contents secrecy (what - like wax envelope seal). Court ordered law enforcement traffic pattern surveillance will give the telephone bill data of who, where, and when.

Media ticket smart card use inside or outside of the US in a spoke receiving US licensed encryption from a US hub can only receive data overseas from a trusted and licensed US source who will be required under proposed US Federal law to use key escrow. A foreign spoke using a media ticket smart card from a US hub will eventually need to get virtual border clearance with that foreign nation. A proposed legislation mutual cryptography cross-licensing trusted nation to nation agreement can be negotiated.

Media ticket smart card use inside the US in a spoke receiving data from an untrusted and unlicensed overseas hub in a foreign country outside of US jurisdiction and without use of proposed cryptography licensing and key escrow laws (or without a trusted nation to nation cryptography cross-licensing agreement with the US) must be electronically policed with "electronic borders." This situation will give foreign nations and terrorists a chance to send strong encryption into the US for military command, control, communications, computers, and coordination (CCCCC or C Five). This unlicensed encryption from unlicensed vendors in foreign countries (e.g. Iraq, Libya, North Korea, PRC, Vietnam) with hubs outside of the US must be electronically

intercepted and monitored or blocked out at the "virtual US border." Suspicious data IP packets from unlicensed overseas vendors or even unlicensed US vendors (having no key escrow provisions) intercepted at "electronic US borders" can be electronically filtered (e.g. optical computers and special cryptography tools) and collected by law enforcement (e.g. NSA, CIA, FBI, state troopers/highway patrol, local police) with a court order for analysis of strong cryptography. Bear in mind that any form of wiretapping without court supervision and US Constitutional law establishes the power of a police state and was a favored tool of the ex-Soviet secret police (KGB), ex-East German secret police (GRU), Nazi secret civilian police (Gestapo), Nazi secret military police (SS). The intercepted illegal packets which are not digitally signed by a licensed US encryption vendor can be "blipped out" with a court order. Bear in mind that key word electronic "blip out" power without court supervision or US Constitutional law exceptions to freedom of religion, freedom of speech, freedom of press, freedom of expression, freedom of assembly, freedom of rightful petition is the police state censoring power to cover-up or conceal the TRUTH.

Allied nations such as the US and NATO with trusted government relations can set up mutual cryptography cross-licensing agreements with any other trusted country. In these agreements one nation such as the US with a US licensed encryption hub restricted to trusted vendors with licensed US key escrow will honor foreign state department, foreign court ordered key escrow requests from a foreign country in which a spoke of a media ticket smart card is in use. This

situation will occur in Hollywood movie distribution with the hub in Hollywood, California and the spokes around the world. Cryptography secret keys for US Copyrighted digital masters distributed worldwide from US hubs will not be surrendered, but, the US will subpoena and surrender to cross-licensed countries the split cryptography keys used for terrorist activities and the illegal distribution of criminal types of information used in racketeering activities (criminal businesses) such as illegal gambling, narcotics distribution, international gang activity, etc.

The mutual situation with the US will arise whereby for example a trusted mutual cryptography cross-licensed nation such as the United Kingdom (UK) having a UK hub with UK licensed key escrow will have a spoke in the US in the form of a citizen/customer using a media ticket smart card. Under the proposed nation to nation cryptography cross-licensing agreements, the UK government will mutually honor US State Department requested foreign key escrow requests from the US government issued by US court order for the clearly illegal or criminal use of UK issued media ticket smart cards in the US.

The goal of preventing terrorist and enemy country to the US use of strong cryptography hardware and software of this invention for foreign invasion and terrorist action in the US by military Command, Control, Communications, Computers, and Coordination (CCCCC or C Fived) is blocked in US jurisdiction by:

- 1). stopping direct and illegal 3rd party sales of this strong cryptography product to terrorist groups and enemy

countries based upon Federal licensing programs for strong cryptography (PROPOSED LEGISLATION) for use entirely in the US or use across US borders.

2). using the 12 legal attributes of cryptography and smart passport cards, smart driver's licenses, smart credit cards, smart debit cards, and media ticket smart cards to allow "electronic US borders" for licensed encryption inside of the US by trusted licensed vendors using mandatory key escrow provisions.

3). (PROPOSED LEGISLATION) Establishing the US licensed cryptography vendor program for trusted corporations with mandatory key escrow.

4). (PROPOSED LEGISLATION) Establishing a mutual cross-licensing program between the US and its trusted allies for honoring court ordered key escrow requests from overseas and for hubs or media servers in one country and spokes or customers in another country.

ALTERNATIVE EMBODIMENTS - DETAILED DESCRIPTION OF

FIGURES, DETAILED OPERATION OF FIGURES OF 1st ALTERNATE EMBODIMENT

Fig. 7 is a circuit block diagram of the 1st alternative embodiment of a cryptographic set-top box for "decrypting" custom encrypted media from high speed digital channels such as cable, phone, "over the air," direct broadcast satellite (DBS) system broadcast, or even "wireless Ethernet" "skip stoned" transmissions.

ADVANTAGES OF ALTERNATIVE EMBODIMENTS - 1st Alternative Embodiment

R. In the 1st alternative embodiment, an object of this invention is to support custom encrypted 'cellular radio' using MPEG X audio layer 3 (MP3) compressed digital audio only, custom encrypted digital standard broadcast (SDTV) and digital high definition "bigscreen" television (HDTV) in digital "over the air" transmitted signals, or else cable distributed digital signals using high speed broadband cable modems, or else phone line distributed signals using high speed asymmetric digital subscriber line (ADSL) broadband modems, or else direct broadcast satellite (DBS) service transmitted signals, or "wireless Ethernet" Institute for Electrical and Electronic Engineers Standard 802.11c (100 Mega bits/second) transmitted "stone skipped" signals, which are all custom decrypted using a cryptographic set-top box with a built-in media ticket smart card reader with an inserted matching media ticket smart card which is further attached to a digital television monitor. A digital television merely has a built-in set-top box of some form. The set-top box may have an additional attached audio/video digital recorder of some form or some level of intelligence.

The HDTV/SDTV signal may have a new from the inventor's cross-referenced invention [REF 512] invention MPEG II extension for a very efficient cryptography "silhouette-like" technique background scene cutting and replacement method of introducing electronic television guide digital data. The digital picture in a picture (PIP) in a

spreadsheet or matrix graphical user interface (GUI) will present the electronic television guide data and select future program recording.

The "over the air" broadcast of (RECOMMENDED FUTURE FCC STANDARD) custom encrypted or "cipher text" standard digital broadcast signals such as High Definition TeleVision (HDTV) or Standard Definition Television (SDTV) signals is supported in my invention with the viewer at home placing his own personal media ticket smart card into the cryptographic set-top box with a built-in media ticket smart card reader. The media ticket smart card will have pre-installed or else customer personal computer (PC) previously downloaded standard broadcast session keys (1-time secret keys which only in this case are shared by more than one viewer with the alternate name of family keys) which are turned into unique personalized play codes for each customer. Each play code will have a matching personalized play count (paid for numbers of plays, -1 for indefinite plays, or counts of free trial plays) for each customer used for digital video recording control of digital to digital copying. The personalization process of turning standard broadcast session keys into unique play codes is done by the authorized media distribution vendor who uses the customer's public key certificate authority (CA) database obtained unique public key to encrypt the session key into a unique play code. The personalized play code is Web down-loaded to the customer's Personal Computer (PC) with an attached media ticket smart card reader and the customer's media ticket smart card inserted. The customer will physically "footprint download" or walking step transfer his media ticket smart card to his

"over the air" cryptographic set-top box with a built-in media ticket smart card reader and a connected digital recorder/cryptographic media player with a built-in media ticket smart card reader. An internet ready set-top box over broadband cable or broadband ADSL phone line (e.g. Web (R) TV) will be able to Internet download directly to the set-top box. The decryption process for the unique customer play count and play code is done in the set-top box/cryptographic media player. First the set-top box/cryptographic media player extracts the customer's unique private key, session key, or 'play code' from his inserted media ticket smart card. The customer private key is used in the accounting process of decrypting the 'play count' or secret key encrypted accounting figure to check for authorized paid for play's greater than 1, -1 for indefinite plays, or counts of free trial plays. A positive accounting verification allows continued extracting of the unique customer 'play code' or session key from the inserted customer media ticket smart card inserted into a built-in media ticket smart card reader. The set-top box/cryptographic media player retrieves from its own tamper resistant memory the authorized media vendor family key and also the unique vendor secret key. The play code is decrypted into a standard session key (1-time secret key shared in this case for standard broadcast only) using the customer's unique private key, the authorized media vendor secret key, and the media vendor family key. The session key is used to decrypt the encrypted broadcast media coming into the set-top box. This will support standard encrypted (not personally encrypted) broadcast media with standard session keys also called shared secret keys or family keys which are turned into personalized play codes and personalized play counts. The play codes

and play counts will be customized to each home viewer through the use of unique public key encryption which only the customer's media ticket smart card holding the unique customer private key can decrypt.

The digitally recorded, standard broadcast, standard encrypted media can be decrypted by any customer with his own media ticket smart card having the appropriate standard broadcast play codes and play counts. The underlying session keys (1-time secret keys which in the standard broadcast case are not unique to each customer) are common. Transfer of the personalized play codes and play counts from one customer's to another customer's media ticket smart card can be done through a special process of the set-top box/cryptographic media player.

One customer's recorded encrypted, standard broadcast, digital media can possibly be decrypted by another customer's media ticket smart card with shared 'play codes' also called family keys or shared secret keys if per chance the two customer's have recorded the same standard broadcast and both have downloaded their own unique play counts and play codes.

The standard broadcast decryption goal of the media ticket smart card in this embodiment will support legal "fair use." The media ticket smart card held personalized play codes and play counts can also be transferred to a customer's back-up media ticket smart card for use in another location such as an automobile or another room. The standard session key encrypted digital HDTV or SDTV broadcast media can be digitally recorded upon a digital versatile disk read/write (DVD/RW (R), DVD+RW (R)), computer hard disk drive (HDD), or compact disk

record once (CD-R) for legal "fair use" copying upon a personal computer.

The media ticket smart card in this embodiment will support legal "first use." The media ticket smart card held play codes and play counts can be legally sold, or given away in entirety by using the cryptographic media player to re-package and transfer the personalized play codes and play counts in the media ticket smart card of the legal owner to the media ticket smart card of another legal owner. This process is explained as the same methods of the "first use" cryptographic key transfer from media ticket smart card A to media ticket smart card B. The recorded encrypted by standard session key digital media will also be transferred and will be useless without the media ticket smart card's matching play codes and play counts.

The goal of an electronic television guide is available through a single digital tuner and the HDTV/SDTV signal using a very efficient (non-MPEG II or non-MPEG IV compliant) cryptography silhouette-like technique for transport of electronic television guide digital data. The electronic television guide data is displayed inside of a digital "picture in a picture (PIP)" by using a spreadsheet or matrix style of graphical user interface (GUI) for current program selection and future program recording. The inventor's related [REF 512] US Patent Pending Application No. 09/999,589, Filing Date Nov. 15, 2001, Filed by Kevin Kawakita, describes this process for the more limited setting of an aircraft digital video recording system (see BACKGROUND - Cross-Reference to My Related Inventions).

ALTERNATIVE EMBODIMENTS - DETAILED DESCRIPTION OF

FIGURES, DETAILED OPERATION OF FIGURES OF 2ND ALTERNATE EMBODIMENT

Fig. 9 is a circuit block diagram of the 2ND alternative embodiment of a cryptographic micro mirror module (MMM) commercial movie theater system (C-MMM).

ADVANTAGES OF ALTERNATIVE EMBODIMENTS - 2nd Alternative Embodiment

S. An advantage of this invention in the 2nd alternative embodiment is to support a high performance, movie cryptographic media player/micro-mirror machine module (MMM) for commercial movie theater use.

CONCLUSION, RAMIFICATIONS AND SCOPE OF INVENTION

A. This invention supports physical distribution of internet "downloaded" custom encrypted digital media limited to digital music, digital movies, electronic newspapers, and electronic books (not including multi-media, computer games, or computer programs which need real-time computer program decryption) (see REFERENCES - NON-PATENT LITERATURE [REF 500] - "The Secure Digital Music Initiative (SDMI)") for "playing" or decryption upon special cryptographic media players.

B. This invention uses only one media ticket smart card per owner with many different digital media distribution vendors.

C. This invention allows the owner's one media ticket smart card to be used with any owner's cryptographic media player [REF 508].

D. This invention stops the use of any unauthorized digital copying of digital media.

E. This invention restricts one digital media distribution company's unencrypted digital masters only to itself and absolutely no other party especially access by any other competing digital media distribution company.

F. This invention allows count controlled play counts or counted decryptions of custom encrypted media including counts of free trial media plays.

G. This invention provides all public key cryptography legal attributes such as:

- 1). authentication (like an exchange of photo ID's or thumbprints)
- 2). encryption/decryption (for privacy)
- 3). integrity (wholeness or non-tampering)
- 4). digital signatures (like handwritten signatures)
- 5). non-repudiation (denying digital signatures)
- 6). authorization (approval using digital signatures and dating or official post marks)
- 7). archiving (storing digitally signed documents in a high integrity environment)
- 8). accessibility (restricting access to authorized users)
- 9). audit trail (recording accesses to information with public key ID's, dates, times, and locations)
- 10). play counts/play codes for counting paid for and authorized personally encrypted digital media plays and for decrypting them
- 11). crypto key splitting and key escrow.

12). crypto key administration and key architectures.

H. This invention supports pass-thru encryption of cryptographic play codes (session keys or 1-time secret keys) and play counts (paid for numbers of plays, -1 for indefinite plays, or counts of free trial plays) for their trip from a media distribution company's central web server over the open internet to a customer's personal computer over wiretappable buses to a secure memory inside of a smart card inserted into a media ticket smart card reader attached to the personal computer.

I. This invention supports physical transfer of encrypted digital media in the form of digital versatile disk read/write, compact disk record once, and FLASH memory cards and also the physical transfer of media ticket smart cards from a customer's personal computer to a cryptographic media player [REF 508].

J. This invention supports pass-thru encryption of cryptographic keys in the form of play codes (session keys or 1-time secret keys) and play counts (paid for numbers of plays, -1 for indefinite plays, counts of free trial plays) from a smart card inserted into a media ticket smart card reader built-into a cryptographic media player [REF 508] for transferring such keys over wiretappable ("red") computer buses to a cryptographic digital signal processor unit having its own tamper resistant non-volatile electrically erasable programmable read only memory which processor is contained inside of the cryptographic media player [REF 508].

Examples are pass-thru, encrypted, transfer of keys from smart cards to media ticket smart card readers (using media ticket smart card reader vendor family keys) to crypto-DSP's (using crypto-DSP vendor family keys) to crypto-CPU's (using crypto-CPU vendor family keys) to crypto-OS's (using crypto-OS family keys) to crypto-software (using crypto-software family keys).

K. This invention supports an optional media ticket smart card citizen/customer authentication triangle between the three points of:

point 1, customer A to (a first means of a passphrase/passcode, a second means of a bio-identification unit such as a digital fingerprint, a third means of a password mixed with pseudorandom noise called salt), to

point 2, media ticket smart card A holding customer A's private keys, encrypted play codes with header, and encrypted play counts with header to prevent the use of stolen media ticket smart cards, to

point 3, cryptographic media player [REF 508].

Any one of the three points which are detected as unauthorized will stop the media ticket smart card read/write process.

L. This invention supports a cryptographic media authentication triangle between the three points of:

point 1, a copy of 1-way transfer of customer session key encrypted digital media A, to

point 2, media ticket smart card holding a customer A's private keys, encrypted play codes with header, and encrypted play counts with header, to

point 3, cryptographic media player [REF 508].

Any one of the three points which are detected as unauthorized will stop the custom encrypted digital media playing process.

M. This invention supports legal "fair use" of US copyrighted encrypted digital media or the archiving of unlimited custom encrypted copies for personal use. The purpose of "fair use" is to allow for recovery in case of accidental damage, theft, fire, flood, natural disaster, legal archiving, disputed legal ownership (as any divorced person will recognise), or one or at most two convenience copies in multiple locations used by the legal owner. Legal "fair use" also supports a home set of media and an auto set of media.

N. This invention supports legal "first use" of US copyrighted encrypted digital media or the right to sell or transfer in entirety the encrypted digital media to another person and transfer only relevant media ticket smart card cryptographic keys to the other person's media ticket smart card.

O. This invention supports lost and stolen media ticket smart cards.

P. This invention supports non-copyrighted commercial material, home produced material, and previously recorded, non-encrypted digital

Copyrighted material by allowing unlimited unencrypted plays of the media.

Q. This invention prevents use of this

strong cryptography system of software and hardware by terrorist forces and countries which are enemies of the United States for military use of Command, Control, Communications, Computers, and Coordination (CCCCC or C Five).

=====

R. In the 1st alternative embodiment, this invention supports custom encrypted 'cellular radio' using MPEG X audio layer 3 (MP3) compressed digital audio, custom encrypted digital standard broadcast (SDTV) and digital high definition television (HDTV) in digital "over the air" transmitted signals, or else cable distributed digital signals using high speed broadband cable modems, or else phone line distributed signals using high speed asymmetric digital subscriber line (ADSL) broadband modems, or else direct broadcast satellite (DBS) service transmitted signals, or else "wireless Ethernet" Institute for Electrical and Electronic Engineers (IEEE) Standard 802.11c (100 Mega bits/second) "skip stoned" transmitted signals which are all custom decrypted using a cryptographic set-top box with a built-in media ticket smart card reader with an inserted matching media ticket smart card which is further attached to a television and audio/video digital recorder.

=====

S. In the 2nd alternative embodiment, this invention supports a high performance, movie cryptographic media player/micro-mirror machine module (MMM) for commercial movie theater use.

...

While my above description contains many specifications, these should not be construed as limitations on the claims of the invention, but rather as an exemplification of some preferred embodiments. Many other alternative embodiments are possible. Different arrangements of computer hardware can be made to support this cryptography architecture and different levels of security can be supported. In addition, the cryptographic digital media can be centrally distributed in physical media along with pre-programmed media ticket smart cards. Use of different underlying ideal public key cryptology algorithms (816) will also support the ideal public key cryptography federated architecture requirements (812). Slightly different sequences in cryptographic protocols or cryptographic algebraic order can produce the same basic results. The entire scope of this invention should be determined by the accompanying legal claims listed just below and not be any specific embodiments thereof.

CLAIMS:

CLAIMS:

We claim:

1. A specific method of or process for doing public key cryptography over an open systems architecture in a totally cryptographically secure manner meant for safeguarding multi-million dollar digital masters which open systems architecture includes existing prior art components and new art invention components defined in the inventor's cross-reference to related patents to give the system components of:

computer hardware components (prior art):

tamper-resistant non-volatile memory used to hold embedded, cryptographic computer programs, cryptographic private keys, cryptographic secret keys, cryptographic session keys, and

often used cryptographic public keys (prior art),

random access memory (prior art),

micro-processors which have wiretappable buses and memory (prior art),

cryptographic embedded micro-processors containing tamper resistant non-volatile memory, random access memory, and embedded firmware for executing cryptographic algorithms over wiretappable ("red") buses and memory and non-wiretappable ("black") buses and cryptographic or secure memory and pass-thru encryption algorithms with means to get the secret data over wiretappable ("red") buses (prior art),

media ticket smart cards containing tamper resistant, non-volatile memory for key storage as part of cryptographic embedded micro-processors (prior art),

media ticket smart card readers containing embedded tamper resistant non-volatile memory for key storage as part of cryptographic embedded micro-processors (prior art),

local area networks (prior art),

internet protocol wide area networks (prior art),

world wide web server computers (prior art),

personal computers (prior art),

personal computer web clients (prior art),

personal computer peripherals (prior art),

cryptographic computer entry devices which include,

cryptographic toggle fields with visible mini-displays with a toggle field into which is entered a passphrase/passcode or in other words a condensed fixed alpha-numeric pseudorandom mix of letters, numbers, and punctuation upon a cryptographic media player device which contains a cryptographic digital signal processor,

cryptographic access codes which include passphrases/passcodes (prior art) typed into a computer keyboard (prior art),

bio-identification with first example means being a customer finger entered into a built-in digital fingerprint reader (prior art) to produce a digitized fingerprint,

personal computer peripheral data storage devices (prior art),

personal computer peripheral data storage media (prior art),

cryptographic hardware secret key algorithm sub-processors inside of cryptographic digital signal processors inside of cryptographic media players,

cryptographic computing units also called cryptographic media players which include:

cryptographic digital signal processors containing cryptographic hardware secret key algorithm sub-processors, tamper resistant non-volatile electrically erasable programmable read only memory, random access memory, analog to digital signal

converters, moving picture electronics group hardware
decompression circuitry for digital audio/video, digital
audio/video signal artificial degradation circuitry, digital to
analog signal converters, and digital signal processing of
digital audio/video signals circuitry,

internal to a personal computer cryptographic media players
which contain cryptographic digital signal processors and access
through prior art personal computer peripherals to external
prior art media ticket smart card readers and personal computer
peripheral data storage media,

external to a personal computer cryptographic media players
which contain cryptographic digital signal processors with
built-in media ticket smart card readers and built-in personal
computer peripheral data storage drives in first example means
of a player being a cryptographic moving picture experts group
standards I audio layer 3 or crypto-mp3 player,

cryptographic media players/high definition television
broadcast receivers/cable digital signal receivers/embedded
personal computer or smart set-top box/digital audio-video
recorders which contain cryptographic digital signal processors
with built-in media ticket smart card readers,

cryptographic media players/micro-mirror modules/theater
projection/theater sound/digital versatile disk read/write drive

units which contain cryptographic digital signal processors with
built-in media ticket smart card readers,

computer software components:

secure operating systems for world wide web server computers
(prior art),

world wide web cryptographic medium download programs (prior
art),

cryptographic mathematics algorithms:

public key cryptography algorithms which create public keys and
private keys, secret key cryptography algorithms which create
secret keys and session keys (1-time secret keys) and also play
counts or access counts or media decryption counts and play codes
(session keys or 1-time secret keys),

hybrid key cryptography algorithms which are combined public key
and private key cryptography algorithms (prior art),

private key and secret key splitting (prior art),

private key and secret key escrow (prior art),

cryptographic keys which are the collective public keys, private
keys, secret keys, session keys (1-time secret keys), play counts,
play codes, passphrases/passcodes (prior art),

computer cryptography protocols (prior art),

pass-thru encryption of cryptographic keys (prior art),

digital media formats (prior art),

computer communications protocols:

transmissions control protocol/internet protocol (prior art)
(TCP/IP),

secure internet protocol layer (prior art),

secure sockets layer (prior art) (SSL),

world wide web server protocols such as hyper-text mark-up
language (prior art) (HTML),

world wide web client protocols such as hyper-text mark-up
language (prior art) (HTML),

and a specific new invention system process of or methods of public key
cryptography comprising of the steps of:

generating of system keys which is the process done by the media
ticket smart card system authority's, party s's, dedicated public key
generation authority, party g, while having absolutely no access to
customer identifications,

generating of media distribution vendor cryptographic keys eventually used in cryptographic digital signal processors for eventual manufacturing into cryptographic media players which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g, while having absolutely no access to customer identifications,

generating of media ticket smart card cryptographic keys which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g,

while having absolutely no access to customer identifications,

distributing of cryptographic digital signal processors which is the process done by the media ticket smart card system authority's, party s's, dedicated public key distribution authority, party d, distributing cryptographic digital signal processors to media distribution vendors for manufacturing into cryptographic media players while having absolutely no access to whole cryptographic keys,

distributing of media ticket smart cards which is the process done by the media ticket smart card system authority's, party s's, dedicated public key distribution authority, party d, distributing media ticket smart cards to media distribution vendors for selling to customers while having absolutely no access to whole cryptographic keys,

escrowing of split cryptographic keys which is the process done by the central public key generation authority, party g, safeguarding the split cryptographic customer keys, and split cryptographic vendor keys

in an entirely secure and confidential manner with legal first means for simple customer identification and lost key recovery, second means for disputed ownership court ordered recovery, and third means for court ordered only use by law enforcement,

layering for a federated cryptography architecture which is the process done by the media ticket smart card system authority, party s, creating a federated architecture of cryptographic authority with 3-layers, a central layer composed of the media ticket smart card system authority, a local layer composed of authorized media distribution companies vN, and a user layer composed of customers,

preparing of play codes and play counts which is the process done by the authorized digital media distribution company, party vN, preparing play codes (session keys or 1-time secret keys), play counts (paid for numbers of plays or counts of free trial plays), and custom encrypted digital media for downloading to each customer,

downloading to customer, party a, which is the process done by the authorized digital media distribution vendor, party vN, using hybrid key cryptographing steps of hybrid key cryptographic digital media distribution from a central media distribution authority hosted on a web server to multiple personal computer based web clients of encrypted play codes (1-time secret keys or session keys) with header and encrypted play counts (paid for counts of plays or decryptions, or else counts of free trial plays) with header for deposit into media ticket smart cards attached to personal computer media ticket smart card readers, and 1-way transfer of custom session key encrypted digital

media for deposit into physical digital media inserted into media drives attached to personal computers,

delivering by foot which is the process done by the customer, party a, of physically transferring both physical custom encrypted digital media and the customer, party a's, programmed media ticket smart cards from the customer's, party a's, personal computer to any person's cryptographic media player with a built-in media ticket smart card reader,

initializing before playing which is the process done by the customer, party a, of preparing any party's cryptographic media player with his own custom encrypted digital media his own media ticket smart card,

authenticating by customer triangle authentication which is the process done by the cryptographic digital signal processor embedded inside of a cryptographic media player which process step may be skipped for low security only when customer time and effort is of the essence,

transferring by pass-thru encryption of cryptographic keys which is the process done by the cryptographic media player to receive encrypted play codes with header and encrypted play counts with header from the media ticket smart card n transferred over wiretappable computer buses to the player's own cryptographic memory for access by its cryptographic digital signal processor,

transferring by pass-thru encryption of cryptographic keys which is the process done by the cryptographic media player's cryptographic digital signal processor to transfer encrypted play codes with header and encrypted play counts with header both with cryptographic digital signal processor incremented sequence counts to the media ticket smart card a transferred over wiretappable computer buses,

authenticating by media triangle authentication which is the process done by a cryptographic media player using digital media triangle authentication using sample reads of real data,

cryptographing using public key cryptography which is the process done by a cryptographic digital signal processor inside of a cryptographic media player using public key cryptography which is the process of using public key cryptography authentication, encryption, and decryption using public keys (puk-n), and private keys (prk-n), stored within tamper resistant non-volatile memory embedded within non-wiretappable ("black") cryptographic computing units in the example of cryptographic digital signal processors,

cryptographing using secret key cryptography which is the process done by a cryptographic digital signal processor inside of a cryptographic media player using secret key cryptography which is the process of using secret key cryptography with a non-wiretappable ("black") bus, cryptographic computing unit in example of a cryptographic digital signal processing unit using secret keys (sek-n), or session keys (ssk-n), stored upon tamper resistant, non-volatile memory,

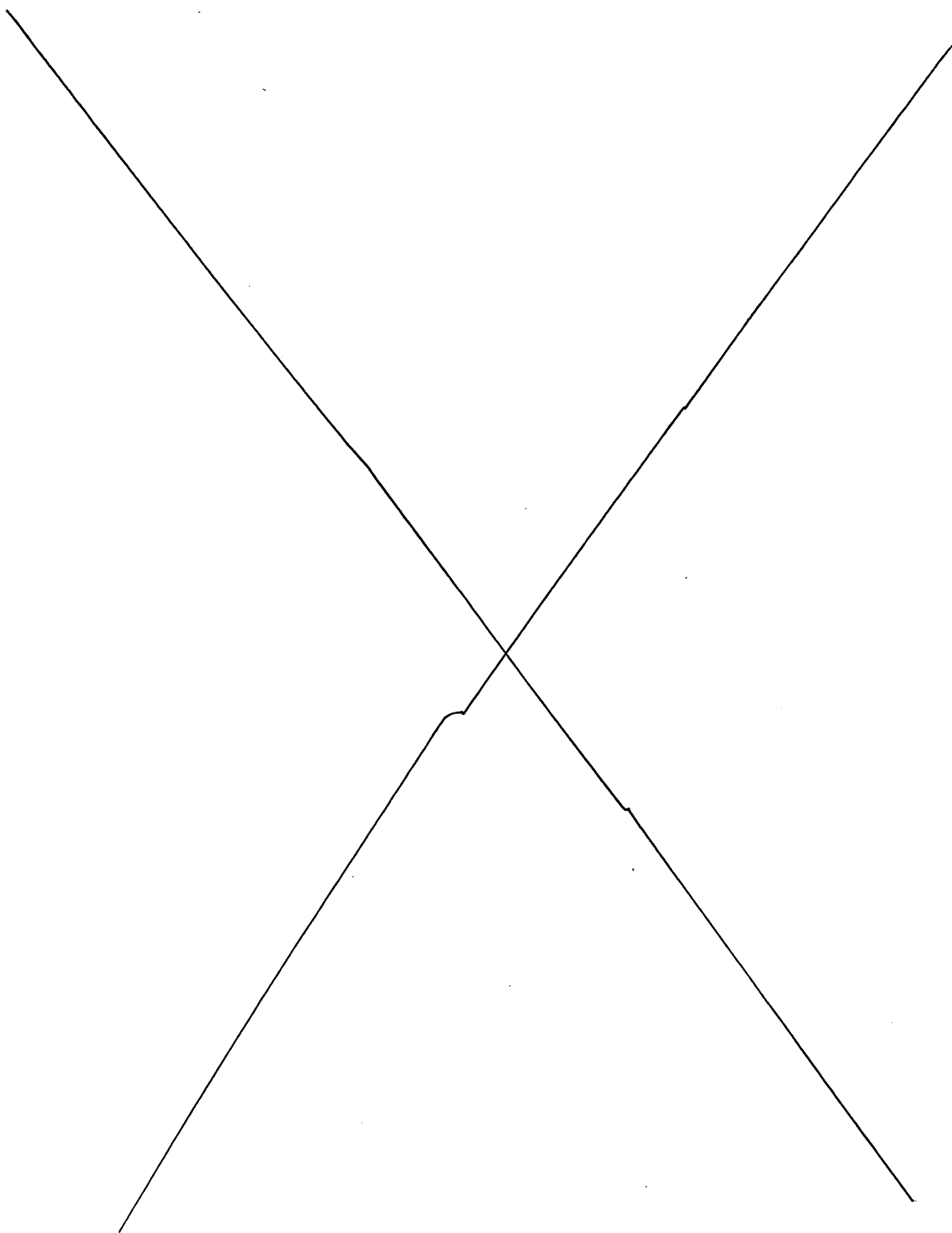
cryptographing using fast hardware session key cryptography which is the process done by a cryptographic digital signal processor inside of a cryptographic media player using hardware secret key cryptography which is the process of using a dedicated hardware secret key sub-processor which is embedded within a secure ("black"), cryptographic digital signal processing unit with access to higher level tamper resistant non-volatile ("black") memory for cryptographic key storage of private keys and secret keys, which hardware secret key sub-processor is much faster than software for secret key cryptography and is intended for fast, secret key cryptography encryption and decryption of block transferred digital media,

cryptographing using hybrid key cryptography which is the process done by a cryptographic digital signal processor inside of a cryptographic media player using hybrid key cryptography which is the process of using hybrid key cryptography which uses public key cryptography to authenticate remote parties, do digital signatures to authenticate digital media and establish media integrity with a remote party, and encrypt one-time secret keys known as session keys (ssk-n), used for only one session, which said session keys are sent to a remote party who decrypts them for storage in his own tamper resistant, non-volatile memory embedded on his black, cryptographic computing unit in the example of a cryptographic digital signal processor and a cryptographic central processing unit which said session keys may be later stored in tamper resistant non-volatile memory embedded in a media ticket smart card where they are referred to as play codes with paid for and authorized play counts.

accounting by the cryptographic digital signal processor which is the process done by the cryptographic media player using hybrid key cryptography digital media playing of 1-way transfer of custom session key encrypted digital media owned by party n in a controlled access manner mostly for financial accounting purposes which uses the play codes (session key or 1-time secret key) and play counts (paid for number of plays or count of free trial plays) contained in media ticket smart cards,

playing by the cryptographic digital signal processor which is the process done by the cryptographic media player using hybrid key cryptography which is the process of using hybrid key cryptography to do digital media playing in a controlled access manner using play codes (session key or 1-time secret keys) and play counts (now contained within registers in the cryptographic digital signal processor and also the hardware secret key decryption device directly used upon the custom encrypted 1-way transfer of custom session key encrypted digital media,

escrowing retrieval of lost, stolen, or disputed ownership media ticket smart cards which is the process done by the customer, party n, which collection of processes of or methods of invention sets systems standards and integrates components into a system which can be used in the future for new forms of internationally standardized cryptography sanctioned by industry tradegroups such as the Recording Industry Association of America (RIAA), the secure digital music initiative (SDMI), and also national standards agencies such as the American National Standards Institute (ANSI), National Institute for Standards and Technology (NIST), or international telegraphy union (ITU).



2. The invention and components of claim 1 whereby the process or methods steps of generating of system keys which is the process done by the media ticket smart card system authority's party s's, dedicated public key generation authority, party g, while having absolutely no access to customer identifications, is accomplished by the sub-steps of:

generating from completely random noise a system family key

(fak-f),

generating of an initialization vector (iv) for use in a system message authentication cipher (mac).

3. The invention and components of claim 2 whereby the process or methods steps of generating of media distribution vendor cryptographic keys eventually used in cryptographic digital signal processors for eventual manufacturing into cryptographic media players which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g, while having absolutely no access to customer identifications, which is accomplished through the sub-steps of:

generating of secret keys (sek-vN), unique to each media distribution vendor, party vN, for later use in embedding a

complete set of media distributor secret keys (sek-v1 to sek-vN), into every cryptographic media player along with a system family key (fak-f), and also for eventual indirectly passing out to each media distribution vendor, party Vn, only his own secret key (sek-vN),

generating of unique vendor private key (prk-vN), public key (puk-vN) pairs, for each media distribution vendor, party vN, for

embedding a system family key (fak-f), a complete set of vendor public keys (puk-v1 to puk-vN), and a complete set of vendor private keys (prk-v1 to prk-vN) into each and every authorized cryptographic media player,

escrowing of all vendor split cryptographic keys generated with a minimum of two central public key escrow authorities, parties en, and other escrow actions.

4. The invention and components of claim 3 whereby the process or methods steps of generating of media ticket smart card cryptographic keys which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g, while having absolutely no access to customer identifications, which is accomplished through the sub-steps of:

generating of public key pairs for different customers, parties a-z (excepting reserved notation use of letters d, e, f, p, s) comprising of private keys (prk-n) and corresponding public keys (puk-n), while having absolutely no access to customer identifications and using prior art public key cryptography,

generating of an incremented, top secret customer index number (cin) also a related public citizen identification number composed of the message digest cipher (mac) of customer index number (mac(cin)) which is publicly printed upon the exterior of each media ticket smart card,

generating of a customer public key database which indexes message digest cipher (mac) of customer index number (mac(cin)) to the blank private key field, to the corresponding public key for passing to the central public key distribution authority, party d,

embedding into media ticket smart card a, a system family key (fak-f), the private key (prk-a) for customer party a indexed by message authentication cipher (mac) of customer index number (mac(cin)) also known as the public customer identification number, also

embedding into media ticket smart card b a system family key (fak-f), the private key (prk-b) for customer party b indexed by message authentication cipher (mac) code of customer index number (mac(cin)), etc.,

generating of an initial media ticket smart card access code such as a passphrase/passcode with storage into a database indexed by message authentication code (mac) of customer index number (mac(cin)) for release to the central public key access code authority, party ea, who will later on release it to the registered customer for initial media ticket smart card use,

handing the media ticket smart cards to the public key distribution authority, party d, and furthermore,

escrowing of all customer split cryptographic keys generated with a minimum of two central public key escrow authorities, parties en, and other escrow actions.

5. The invention and components of claim 4 whereby the process of or method of steps to do distributing of cryptographic digital signal processors which is the process done by the media ticket smart card system authority's, party s's, dedicated public key distribution authority, party d, distributing cryptographic digital signal processors to authorized media distribution vendors for eventual manufacturing into cryptographic media players while having absolutely no access to whole cryptographic keys which consists of the sub-steps of:

distributing of cryptographic digital signal processors in a physically secure transport and audit trailed chain by the central

public key distribution authority, party d, only to authorized media distribution vendors, parties Vn,

manufacturing by the authorized media distribution vendors, parties Vn, of cryptographic digital signal processors into different forms of cryptographic media players with various specialized functions and applications,

retailing by the authorized media distribution vendors of cryptographic media players with various specialized functions and applications to consumers.

6. The invention and components of claim 5 whereby the process of or method of steps to do distributing of media ticket smart cards which is the process done by the media ticket smart card system authority's, party s's, dedicated public key distribution authority, party d, distributing media ticket smart cards to media distribution vendors while having absolutely no access to whole cryptographic keys which consists of the sub-steps of:

assigning of media ticket smart cards eventually to media ticket smart card users which is the sub-step done by the central public key distribution authority, party d, assigning media ticket smart cards received from the public key generating authority from the methods of claim 4, to authorized media distribution vendors and eventually to media ticket smart card customers who will register names, addresses, etc. which can be mapped into a database by the

publicly known message authentication cipher of customer index number (mac(cin)) on the exterior of the media ticket smart card,

imprinting of media ticket smart cards which is the sub-step done by the central public key distribution authority, party d, imprinting the media ticket smart cards with customer identification which fields are accessed by using the media ticket smart card customer identification field family key obtained from the public key generating authority,

distributing of media ticket smart cards to customers which is the sub-step done by the central public key distribution authority, party d, giving the media ticket smart cards to authorized media distribution vendors, parties vN, for selling the media ticket smart cards to media ticket smart card customers through an appropriate secure physical channel such a retail store, express mail, and registered mail which media ticket smart cards are useless without registration with the central public key distribution authority, party d, and receiving of a temporary media ticket smart card access codes unless a wildcard access code was programmed by the public key generating authority,

possessing of media ticket smart cards which is the sub-step done by the customer, party a, receiving a media ticket smart card with exterior message authentication code (mac) of customer index number (mac(cin)) and registering the media ticket smart card at the retail store or by mailing back in a registration card with customer n's name, address, phone number, e-mail address, etc. and

public customer identification number which will allow the central public key distribution authority, party d, to use its customer database to map such identifications to the customer's public key,

publishing of public keys which is the sub-step done by the central public key distribution authority, party d, openly publishing using internet protocol over the internet from a web server all public keys and appropriate user identities such as name and message authentication code of customer index number (mac(cin)),

handling of media ticket smart card temporary user access codes which is the sub-step done by the central public key distribution authority, party d, handing only customer name, mailing address, and phone number indexed by a message authentication cipher of the secret customer index number to the public key access code authority which public key access code authority already has from process 2 the media ticket smart card temporary access codes also indexed by the same message authentication cipher of the secret customer index number, furthermore, the public key access code authority has no media ticket smart cards or media ticket smart card reader family key from the claims of process 2,

distributing of media ticket smart card temporary user access codes which is the sub-step done by the public key access code authority, party ea, matching customer names, mailing address, and phone number to temporary media ticket smart card access codes in order to mail out media ticket smart card temporary access codes to

media ticket smart card users, afterwhich the public key access
code authority promptly destroys all information it has used except
for confirmation of the mailing.

7. The invention and components of claim 6 whereby the process of or method of steps to do escrowing of key split cryptographic keys which is the process done by the smart media system authority's, party s's, dedicated public key escrow authority, party e, and also the dedicated public key access code authority, party ea, which both have knowledge of split cryptographic keys, but, absolutely no knowledge of customer identifications through the sub-steps of:

receiving of the split cryptographic customer key database of customer private keys, PrK-n (a minimum of a front half and a back half key) and also the split cryptographic vendor key database of vendor private keys, prk-vN, and vendor secret keys, sek-Vn (a minimum of a front half and a back half key) which is the sub-step done by the central public key escrow authorities, parties en, receiving split key databases from the central public key generation authority, party g,

collaborating prevention which is keeping separate the key split customer and vendor cryptographic keys between a minimum of two (for a front half of key and a back half of key) independent key escrow authorities, parties En who have absolutely no access to customer identifications,

receiving of media ticket smart card initial media ticket smart card access codes which is the sub-step done by the independent public key access code authority, party ea, receiving from the

public key generation authority, party g, a database of initial media ticket smart card access codes indexed by message authentication code of customer index number ($\text{mac}(\text{cin})$) and also receiving from the central public key distribution authority, party d, customer names, mailing addresses, and e-mail accounts also indexed by message authentication code of customer index number ($\text{mac}(\text{cin})$),

distributing of media ticket smart card initial access codes which is the sub-step done by the public key access code authority, party ea, secure means transmitting through first example means of certified mailing or secure e-mailing to customers of the initial access codes, afterwhich receiving back confirmation it promptly destroys all knowledge of customer identifications.

8. The invention and components of claim 7 whereby the process of or method of steps to do layering for a federated cryptography architecture which is the process done by the media ticket smart card system authority, party s, through the sub-steps of:

layering into 3-layers of a federated architecture of cryptographic authority:

a central layer composed of media ticket smart card system authority,

a local layer composed of authorized media distribution companies Vn, and

a user layer composed of customers.

9. The invention and components of claim 8 whereby the process of or method of steps to do preparing of play codes and play counts which is the process done by the authorized digital media distribution company, party vN, through the sub-steps of:

preparing of the media header for each download media session which is:

unique vendor and customer encrypted play code with media header (and sequence numbers):

```
{  
  
    vendor identification number (mac(vin)) = message  
    authentication cipher (mac) of top secret vendor index  
    number (vin),  
  
    session identification number,  
  
    customer A public key encrypted(  
  
        vendor secret key encrypted(  
  
            vendor digitally signed {play code  
  
                (session key or 1-time secret key),  
  
                vendor sequence number,  
  
                message authentication code of customer  
  
                    identification number})),  
  
    customer (family key) sequence number,
```

```
} = temp-9a,
```

unique vendor and customer encrypted play count with media header (and sequence numbers):

```
{  
  
    vendor identification number (mac(vin)) = message  
    authentication cipher (mac) of top secret vendor index  
    number (vin),  
  
    session identification number,  
  
    customer A public key encrypted(  
  
        vendor secret key encrypted(  
  
            vendor digitally signed {play count  
  
                (paid for numbers of plays,  
  
                -1 for infinite plays,  
  
                count of free trial plays),  
  
                vendor sequence number,  
  
                message authentication code of  
  
                customer identification number})),  
  
    customer (family key) sequence number,  
  
} = temp-9b,
```

encrypting of the play codes (session keys or 1-time secret keys) which are truly random numbers in a desired range with header is a

process of first, the vendor digitally signs (prk-vN) the decrypted play code, and then attaches the header and sequence number and secondly, the vendor three-way encrypts the result with the sequence of first encryption with the secret key of the vendor, sek-vN, second encryption, with the public key of receiving customer, party a, puK-a, third encryption with the system family key, fak-f, for pass-thru encryption:

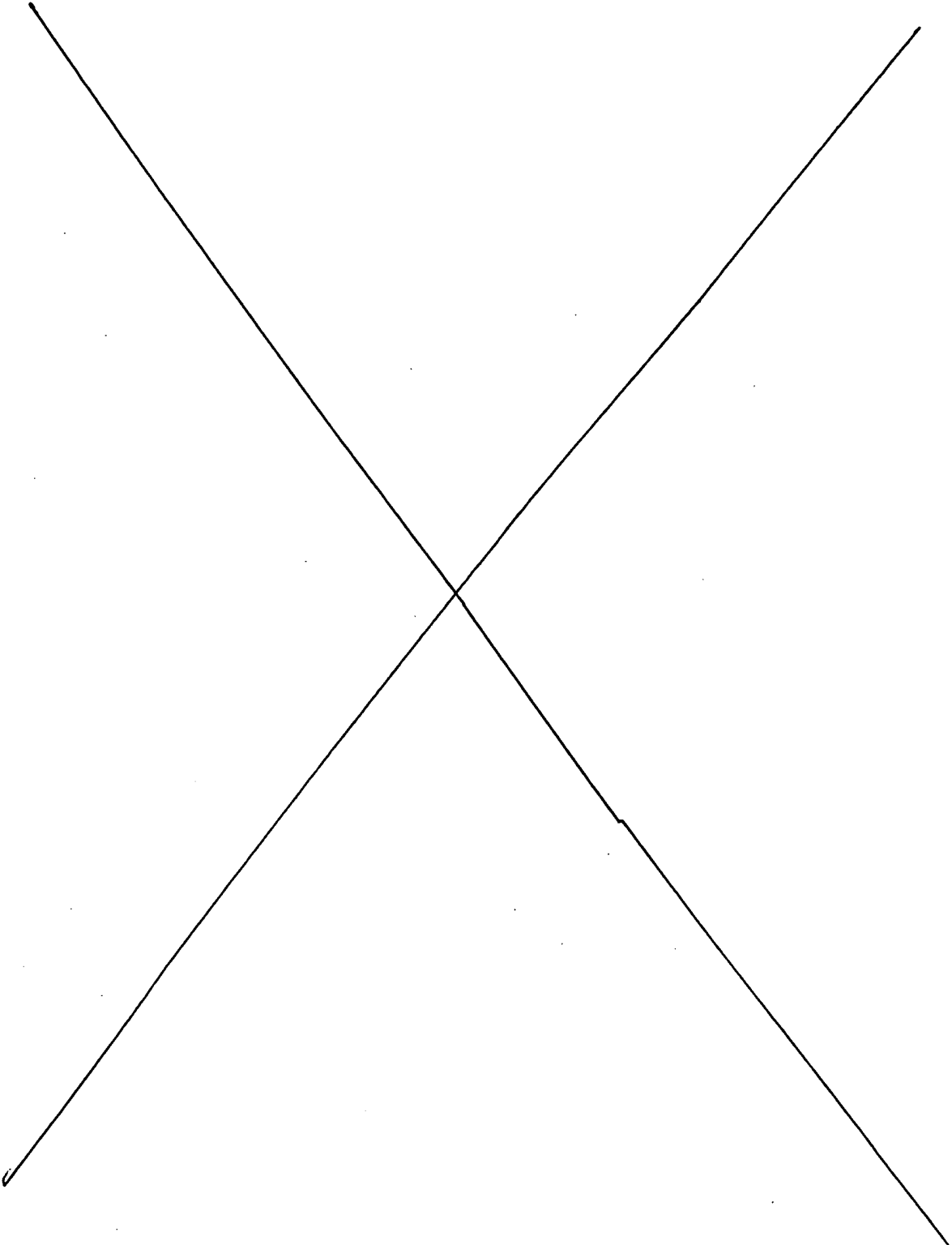
vN-fak-f(temp-9a)

= pass-thru encrypted play code with header (and sequence numbers),

furthermore,

the sequence number is needed to prevent recorded replay attacks on wiretappable buses of pass-thru encrypted signals inside of the cryptographic media player, furthermore, the sequence number can only be incremented by a party with the vendor secret key (sek-vN), customer private key (prk-n), and system family key (fak-f) who are the party g for any vendor, the party vN only for his own play codes and play counts, or the cryptographic media player, party p, for any vendor which player has a collection of all vendor secret keys (sek-v1 to vN) and a collection of all vendor private keys (prk-v1 to vN), furthermore, used in key ownership re-assignment operations by the cryptographic digital signal processor (C-DSP) in the cryptographic media player, party P, furthermore, the customer (family key) sequence number is used in media ticket smart card loop-back operations, furthermore, the player can also check the vendor digital signature,

and can obtain the customer a's private key (prk-a) and public key (puk-a) from customer's inserted media ticket smart card a,



encrypting of play counts (counts of paid for numbers of
play, 1 for indefinite plays, or counts of free trial plays)
which are encrypted by the sequence of:

vN-fak-vN(temp-9b)

= pass-thru encrypted play count with header (and sequence
numbers).

10. The invention and components of claim 9 whereby the process of or method of steps to do downloading to customer, party a, using digital media distribution which is the process done by the media distribution vendor, party vN, through the sub-steps of:

accounting by credit card if payment for the custom encrypted digital media is due to the media distribution vendor,

cryptographing from a media distribution vendor's secure media web server to a customer a's personal computer using prior art, commercial, low security, secure sockets layer hybrid key cryptography of already pass-thru encrypted with incremented sequence numbers (to prevent recorded replay attacks), encrypted play codes (1-time secret keys or session keys) with header and encrypted play counts (paid for counts of plays or decryptions or else counts of free trial plays) with header for deposit into media ticket smart cards attached to built-in media ticket smart card readers,

cryptographing from a media distribution vendor's secure media web server to a customer a's personal computer using prior art, commercial, low security, secure sockets layer hybrid key cryptography of already custom, encrypted digital media for deposit into physical media inserted into built-in media drives.

11. The invention and components of claim 10 whereby the process of or method of steps to do delivering by foot which is the process done by the customer, party a, which consists of the sub-steps of:

transporting his own custom encrypted digital media to any cryptographic media player along with his own media ticket smart card a,

inserting of his own custom encrypted digital media and his own media ticket smart card a into any cryptographic media player with a built-in media ticket smart card reader.

12. The invention and components of claim 11 whereby the process of or method of steps to do initializing before playing which is the process done by the cryptographic media processor inside of any authorized cryptographic media player accomplished by the sub-steps of:

verifying of insertion by some customer of some custom session key (1-time secret key) encrypted media into the cryptographic media player's media drive,

verifying of insertion by some customer of some media ticket smart card a into the built-in media ticket smart card reader on the cryptographic media player,

prompting by the cryptographic media player of some customer to enter his access code through a first means such as a built-in cryptographic alphanumeric toggle field with liquid crystal display with a minimum of one-line display, or through a second means of a computer keyboard, or through a third means of a biological identification (bio-id) reader with example means being a digital fingerprint reader.

13. The invention and components of claim 12 whereby the process of or method of steps to do authenticating by customer triangle authentication which is the process done by the cryptographic digital signal processor embedded inside of the cryptographic media player accomplished through the sub-steps of:

identifying of a low security application and skipping this sub-process step for low security applications only where customer time and effort is critical,

initializing of cryptographic media player through the process of claim 12,

transferring media ticket smart card access codes such as a first example means of passphrases/passcodes customer entered into a first means of a built-in cryptographic media player toggle field with a minimum of one-line display, and a second example means of being customer entered into a computer keyboard on a personal computer, and a third example means of a customer finger entered into a built-in bio-identification unit such as a digital fingerprint reader, which all example means are transferred to a cryptographic digital signal processing unit which is embedded inside of the cryptographic media player,

encrypting using pass-thru encryption and the system family key, fak-f, by the media ticket smart card of the customer's media

ticket smart card access code in example means being passphrases/passcodes, passwords having automatically mixed in pseudorandom noise called salt, and bio-identification such as a digital fingerprint with an added incremented sequence number which is automatically added by the authorized media distribution vendor and the authorized cryptographic media player in order to prevent recorded replay attacks,

transferring of the pass-thru encrypted media ticket smart card access code in first example means being passphrases/passcodes, and second example means being passwords with vowels automatically replaced by pseudo-random noise, and a third example means being bio-identification such as a digital fingerprint transmitted over wiretappable ("red") computer buses from the media ticket smart card to the cryptographic digital signal processor,

decrypting using pass-thru encryption and the system family key, fak-f, by the cryptographic media player of the customer's media ticket smart card access code in first example means being passphrases/passcodes, passwords with automatically mixed in pseudorandom noise called salt, and second example means being bio-identification such as digital fingerprints with added incremented sequence number used to prevent recorded replay attacks,

verifying against recorded replay attacks by the cryptographic media player by checking for an incremented sequence number which can only be incremented by the media distribution vendor or else any cryptographic media player over the previous recorded sequence

number in local cryptographic memory which is the retrieved previous access of the same media ticket smart card access code received from the media ticket smart card, incremented of sequence number by the cryptographic media player,

doing the reverse steps to transfer the encrypted access code with incremented sequence number from the cryptographic media player back to the media ticket smart card,

authenticating by customer triangle authentication of the following points:

point 1 of customer, party a, access code comprising of a first example means of a passphrase/passcode, a password with automatic random noise called salt added to the entry, and a second example means of a bio-identification such as a digital fingerprint, to

point 2 of media ticket smart card a, to

point 3 of authorized cryptographic media player.

14. The invention and components of claim 13 whereby the process of or method of steps to do transferring by pass-thru encryption which is the process done by the cryptographic digital signal processor embedded inside of the cryptographic media player sending a request to the media ticket smart card to transfer back cryptographic keys or an error status comprising of the sub-steps of:

 authenticating using customer triangle authentication which is the process of claim 13,

 requesting by the cryptographic digital signal processor sent to the media ticket smart card a request key message pass-thru encrypted with the system family key (fak-f),

 transferring by the media ticket smart card n to the cryptographic digital signal processor of the return message of the requested cryptographic keys comprising of customer private key (prk-n), encrypted play codes (session keys or 1-time secret keys) with header, encrypted play counts (paid for numbers of plays, -1 for infinite plays, or counts of free trial plays) with header all with sequence numbers to prevent recorded replay attacks,

 decrypting by the cryptographic digital signal processor of the returned pass-thru encrypted cryptographic keys from the media ticket smart card using its trusted family key to decrypt the pass-thru encrypted cryptographic keys,

verifying by the cryptographic digital signal processor of incremented sequence numbers in the keys returned from the media ticket smart card in order to prevent recorded replay attacks which is the sub-step done by the cryptographic digital signal processor using its locally cryptographically stored trusted family key (fak-f), customer private key (prk-n) retrieved from the customer's media ticket smart card, vendor public key (puk-vN), and vendor secret key (sek-vN) retrieved from local cryptographic memory, to decrypt the sequence numbers and check for an incremented value over the previous values stored in local cryptographic memory (the cryptographic media player will increment the sequence number before storage as only an authorized media distribution vendor or any cryptographic media player can alter a sequence number),

storing by the cryptographic digital signal processor in its own local cryptographic memory of the media ticket smart card's verified and decrypted cryptographic keys composed of the customer's private key, PrK-n, decrypted play count with header, decrypted play code with header in its own local tamper resistant non-volatile memory, this process must be followed by an

incrementing of sequence number function done by the cryptographic digital signal processor, and an opposite direction transferring function by the cryptographic digital signal processor to the media ticket smart card of the updated cryptographic keys with incremented sequence number in order to avoid their rejected use in the future.

15. The invention and components of claim 14 whereby the process of or method of steps to do transferring by pass-thru encryption which is the process done by the cryptographic digital signal processor in the cryptographic media player transferring cryptographic keys from itself to the media ticket smart card with a return error status comprising of the sub-steps of:

transferring by pass-thru encryption by the cryptographic digital signal processor to the media ticket smart card which is the process of transferring cryptographic keys comprising of customer private key (prk-n), encrypted play codes with header, encrypted play counts with header, all with already incremented customer (family key) sequence numbers from itself to the media ticket smart card,

decrypting of pass-thru encrypted cryptographic keys by the media ticket smart card which is the process done using its trusted family key to decrypt the pass-thru encrypted cryptographic keys from the cryptographic digital signal processor,

verifying of incremented customer (family key) sequence numbers to prevent recorded replay attacks which is the sub-step done by the cryptographic micro-processor embedded inside of the media ticket smart card using its local cryptographically stored trusted family key, fak-f, to pass-thru decrypt the pass-thru encrypted play code with header (and sequence numbers):

removing the message authentication code of the vendor identification number,

removing the session identification number,

removing the customer (family key) sequence number,

leaving the last to first by initial vendor media distribution center operation, customer public key encrypted,

vendor secret key encrypted, vendor digitally signed both of play code and vendor sequence number,

checking by the media ticket smart card for an incremented customer (family key) sequence number to prevent a recorded replay attack,

storing of cryptographic keys which is the sub-step done by the cryptographic micro-processor embedded inside of the media ticket smart card storing the pass-thru decrypted keys including the customer's private key, PrK-n, decrypted updated play count with header, decrypted play code with header all with updated sequence numbers into its own local tamper resistant non-volatile memory,

returning of error status from the media ticket smart card back to the cryptographic media processor which are the sub-steps of the media ticket smart card composing an error warning or normal status warning with the looped back sequence number which is pass-thru encrypted and returned to the cryptographic digital signal processor.

16. The invention and components of claim 15 whereby the process of or method of steps to do authenticating by media triangle authentication which is the process done by a cryptographic digital signal processor within a cryptographic media player accomplished through the sub-steps of:

initializing by the customer, party a, of the cryptographic digital signal processor through the process of claim 12,

authenticating by the cryptographic digital signal processor of customer triangle authentication through the process of claim 13,

reading by the cryptographic digital signal processor of the custom encrypted digital media to obtain the vendor identification number and session identification number of the particular media indexed by cryptographic digital signal processor identification number,

{

vendor identification number (mac(vin)),

session identification number,

play code encrypted digital media,

}

encrypting by the cryptographic digital signal processor using pass-thru encryption and the system family key, fak-f, of the

media's vendor identification number and session identification number with an incremented sequence number to prevent recorded replay attacks,

transferring by the cryptographic digital signal processor to the media ticket smart card inserted into a built-in media ticket smart card reader of the media's pass-thru encrypted vendor identification number and session identification number with an incremented sequence number,

decrypting by the media ticket smart card using pass-thru decryption using the system family key, fak-f, of the media's vendor identification number and session identification number with an incremented sequence number to prevent recorded replay attacks,

verifying by the media ticket smart card against recorded replay attacks in the decrypted data by checking for an incremented sequence number over the local cryptographical memory stored previous recorded sequence number access indexed with the same cryptographic digital signal processor identification number,

retrieving by the media ticket smart card n from its local cryptographic memory in the vendor identification number table, the session identification number of the matching encrypted play codes with header and encrypted play counts with header plus its own customer private key, prk-a,

notifying by the media ticket smart card back to the cryptographic digital signal processor of a custom encrypted digital media to media ticket smart card mismatch error status going back if the vendor identification number and session identification number search produces no matches in local cryptographic memory,

decrypting by the cryptographic digital signal processor using pass-thru decryption with the system family key, fak-f, and decryption using the vendor public key, puk-vN, and vendor secret key, sek-vN, out of the set of all vendor public keys and vendor secret keys retrieved from local cryptographic memory by the cryptographic digital signal processor used upon the customer's encrypted play code with header, play count with header, and private key, prk-a, with sequence number to prevent recorded replay attacks,

verifying against recorded replay attacks by the cryptographic digital signal processor by checking for an incremented sequence number over the previous recorded sequence number access of the same media ticket smart card held in local cryptographic memory,

incrementing by the cryptographic digital signal processor of the customer (family key) sequence number received from the media ticket smart card,

encrypting by the cryptographic digital signal processor using pass-thru encryption and the system family key, fak-f, of the media ticket smart card's retrieved encrypted private key, prk-a,

encrypted play codes with header, and encrypted play counts with header, all with an incremented sequence number to prevent recorded replay attacks,

transferring using pass-thru encryption by the cryptographic digital signal processor to the media ticket smart card of the updated cryptographic keys comprising of customer a's private key, prk-a, encrypted play codes (session keys or 1-time secret keys) with header and encrypted play counts (paid for numbers of plays, - 1 for infinite plays, or counts of free trial plays) with header and all with sequence numbers by the process of claim 15,

authenticating of the media triangle authentication by the cryptographic digital signal processor which is the sub-step done by the cryptographic digital signal processor inside of the cryptographic media player decrypting a sample known test pattern of the digital media by using the decrypted play code (session key or 1-time secret key) stored inside of local cryptographic memory in the cryptographic digital signal processor also with using the vendor's public key, puk-vN, and vendor's secret key, sek-vN, in order to undo the encryption of process 9, by the sub-steps of:

unique vendor and customer play count with media header (and sequence number) is:

```
(  
  
    vendor identification number (mac(vin)),  
  
    session identification number,  
  
    customer A public key encrypted  
  
        (vendor secret key encrrypted  
  
            (vendor private key digitally signed(  
  
                play count, sequence number)))  
  
    customer (family key) sequence number,  
  
    ) = temp-16a,  
  
    vendor pass-thru encrypted play count with media header (and  
    sequence numbers) is:  
  
    family key (temp-16a) = temp-16b,
```

unique vendor and customer play code with media header (and sequence numbers) is:

```
(  
  
    vendor identification number (mac(vin)),  
  
    session identification number,  
  
    customer A public key encrypted  
  
        (vendor secret key encrypted  
  
            (vendor private key digitally signed  
  
                {play code, sequence number}))  
  
    customer (family key) sequence number,  
  
    )  
  
    ) = temp-16c,  
  
    vendor family key encrypted or pass-thru encrypted play code with  
media header and sequence number is:
```

family key (temp-16c) = temp-16d,

and then using the decrypted play code also known as a session key or 1-time secret key for decrypting the custom encrypted digital

media which known sample data area will only decrypt properly to a known test pattern with the proper untampered with play code,

authenticating with media triangle authentication by the cryptographic digital signal processor of the following points:

point 1 of custom, encrypted digital media a, to

point 2 of media ticket smart card a, to

point 3 of authorized cryptographic media player.

17. The invention and components of claim 16 whereby the process of or method of steps to do cryptographing using public key cryptography which is the process done by a cryptographic digital signal processor within a cryptographic media player accomplished through the sub-steps of:

 authenticating of play code digitally signed by the authorized media distribution vendor's private key to the cryptographic digital signal processor which is the sub-step done by the cryptographic digital signal processor which holds the complete public key set of all authorized media distribution vendors retrieving the play code from the media ticket smart card a and using the correct vendor public key to decrypt the session key which was digitally signed by the vendor private key to reveal the decrypted session key ready for use on the custom encrypted digital media.

18. The invention or components of claim 17 whereby the process of or method of steps to do cryptographing using secret key cryptography which is the process done in a cryptographic digital signal processor within a cryptographic media player through the sub-steps of:

decrypting of the custom encrypted digital media which is the sub-step done by the cryptographic digital signal processor using the decrypted session key (1-time secret key) for fast, software secret key cryptography without use of a fast hardware secret key unit by loading it into the cryptographic digital signal processor's which can software decrypt the custom encrypted digital media.

19. The invention and components of claim 18 whereby the process of or method of steps to do cryptographing using fast hardware session key cryptography which is the process done in a cryptographic digital signal processor within a cryptographic media player accomplished through the sub-steps of:

decrypting of the custom encrypted digital media which is the sub-step done by the cryptographic digital signal processor using the decrypted session key (1-time secret key) for fast, hardware secret key cryptography by loading it into the cryptographic digital signal processor's hardware secret key unit which can fast hardware decrypt the custom encrypted digital media.

20. The invention and components of claim 19 whereby the process of or method of steps to do cryptographing using hybrid key cryptography which is the process done in a cryptographic digital signal processor within a cryptographic media player accomplished through the sub-steps of:

 authenticating of play code digitally signed by the authorized media distribution vendor's private key to the cryptographic digital signal processor which is the sub-step done by the cryptographic digital signal processor which holds the complete public key set of all authorized media distribution vendors retrieving the play code from the media ticket smart card a and using the correct vendor public key to decrypt the session key which was digitally signed by the vendor private key to reveal the decrypted session key ready for use on the custom encrypted digital media,

 decrypting of the custom encrypted digital media which is the sub-step done by the cryptographic digital signal processor using the decrypted session key (1-time secret key) for fast, hardware secret key cryptography by loading it into the cryptographic digital signal processor's hardware secret key unit which can fast hardware decrypt the custom encrypted digital media.

21. The invention and components of claim 20 whereby the process of or method of steps to do accounting of play codes and play counts which is the process done by the cryptographic digital signal processor within a cryptographic digital media player accomplished through the sub-steps of:

authenticating step done in high security applications which sub-process step is simply skipped in low security applications for citizen/customer time and effort consideration, of the customer triangle authentication using the process of claim 13 of:

point 1 of customer a, to

point 2 of media ticket smart card a, to

point 3 of cryptographic media player,

authenticating of the media triangle authentication by the process of claim 16 consisting of:

point 1 of 1-way transfer of custom session key encrypted digital media, to

point 2 of media ticket smart card a with appropriate play

codes and play counts, to

point 3 of cryptographic media player,

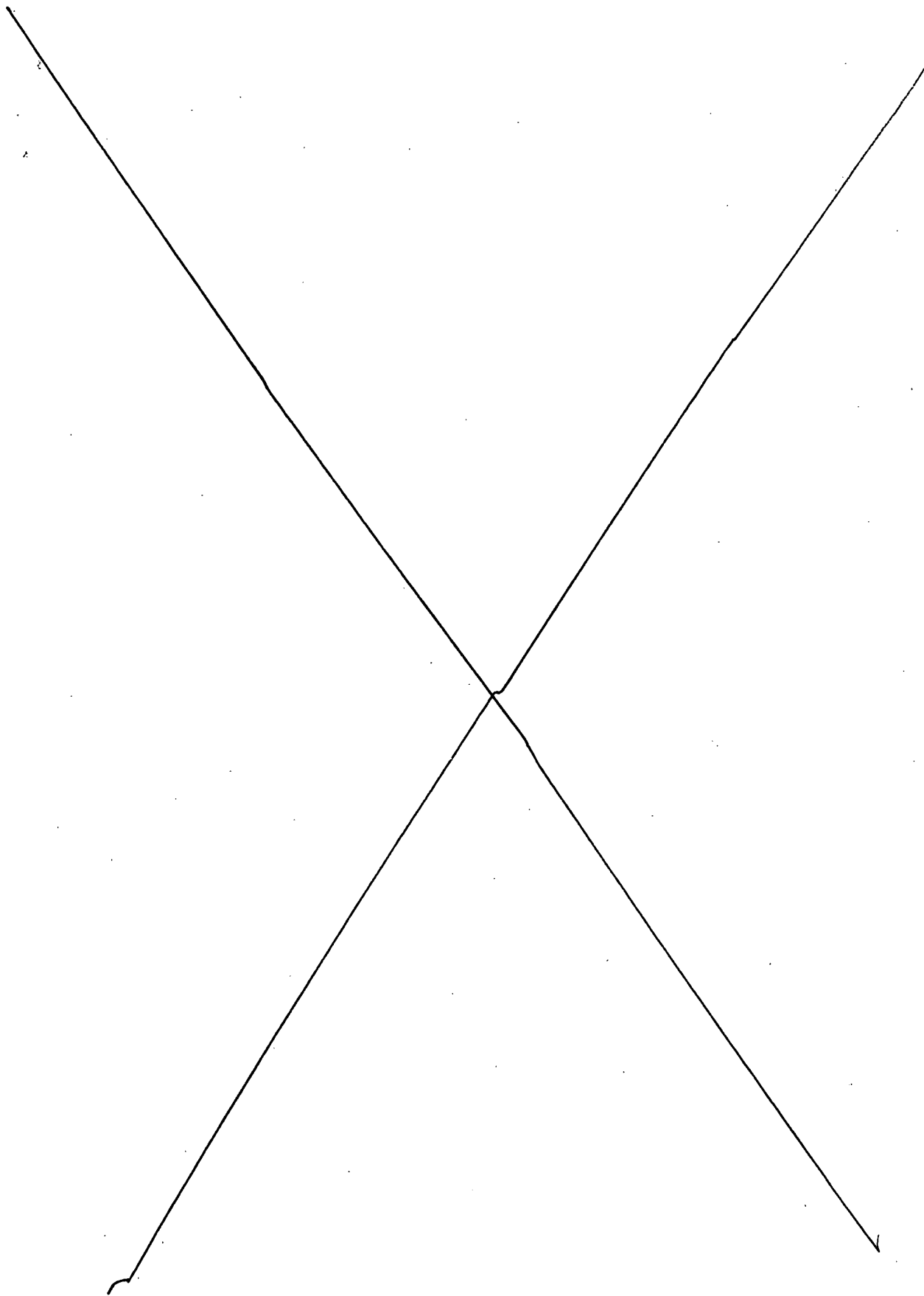
notifying of the customer of any errors in the above two sub-steps, transferring by the media ticket smart card to the cryptographic digital signal processor of the pass-thru encrypted cryptographic keys comprising of customer private key (PrK-n), play count with header, and play code with header all with sequence numbers using the process of claim 14,

verifying of decrypted play count greater than one which is the sub-step done by a cryptographic digital signal processor inside of a cryptographic media player checking the obtained decrypted play count for a greater than one number indicating authorized and paid for plays remaining while a -1 value for a count can be a means of indicating an infinite number of plays,

decrementing of play count which is the sub-step done by the cryptographic digital signal processor unit of decrementing of the play count,

incrementing of customer (family key) sequence number by the cryptographic digital signal processor to prevent recorded replay attacks,

transferring by the cryptographic digital signal processor to the media ticket smart card of the pass-thru encrypted cryptographic keys comprising of customer private key (PrK-n), updated play count with header, and play code with header all with incremented sequence numbers using the process of claim 15.



22. The invention and components of claim 21 whereby the process of or method of steps to do playing of custom encrypted digital media which is the process done by the cryptographic digital signal processor within a cryptographic media player accomplished through the sub-steps of:

detecting of non-copyrighted commercial or home-made material with an absense of encryption will allow hardware decompression of standard form compressed digital media, artificial digital degradation, and digital to analog conversion for analog output while skipping the following sub-steps,

accounting by the cryptographic digital signal processor of the custom encrypted digital media using the process of claim 21,

cryptographing by the cryptographic digital signal processor using hybrid key cryptography playing of the custom encrypted digital media using the process of claim 20.

23. The invention and components of claim 22 whereby the process of or method of steps to do escrowing retrieval of lost, stolen, or disputed media ticket smart cards by the customer such that existing custom encrypted media can still be used which is the process done by the customer, party a, accomplished through the sub-steps of:

reporting of lost, stolen, or disputed legal ownership media ticket smart cards by the customer, party a, to the central public key distribution authority, party d,

cancelling of the existing card by the public key distribution authority, party d, in its customer database,

retrieving by the central public key distribution authority, party d, from the central public key escrow authorities, parties en, of the old customer public key pair,

issuing of a new card by the public key distribution authority, party d, with a new customer public key pair,

retrieving by the central public key distribution authority, party d, from all media distribution vendors, parties vN, of existing partially encrypted customer's, party a's, play codes and play counts stored in computer database (which will not have the latest play count of the lost card which does not matter for infinite plays or free trial plays and financial compensation can be made for finite play counts) from all download sessions which

can be restored with customer's, party a's, new public keys done by the process of:

```
d-prk-a-old(

    remove MAC(VIN),

    remove session identification number,

    remove customer (family key) sequence number,

    (d-fak-f

        (pass-thru encrypted play code with

            header (and sequence numbers)

        ),

    )) = temp-23a,

d-prk-a-old (

    remove MAC(VIN),

    remove session identification number,

    remove customer (family key) sequence number,

    (d-fak-f

        (pass-thru encrypted play count (with

            sequence numbers)

        ),

    )) = temp-23b,
```

imprinting the customer's, party a's, old play codes and play counts into the new media ticket smart card,

d-fak-f(

MAC(VIN),

session identification number,

d-puk-a-new(temp-23a),

customer (family key) sequence number + 1) =

(new encrypted play code with header

(and sequence numbers),

d-fak-f(

MAC(VIN),

session identification number,

d-puk-a-new(temp-23b),

customer (family key) sequence number + 1) =

(new encrypted play count with header (and sequence

numbers),

delivering of the reconstructed, new media ticket smart card to the customer which should work with existing custom encrypted media

and it will still work with the lost, stolen, or legally disputed
old media ticket smart card.

24. The invention and components of claim 23 whereby the process of or method of steps to do legal re-assigning of play code and play count ownership from media ticket smart A of owner A to media ticket smart card B of owner B which is legally called "first use" involving US Copyrighted digital media which is accomplished through the sub-steps of:

inserting of media ticket smart card A into the cryptographic digital signal processor (C-DSP) inside of a cryptographic media player (e.g. C-MP3 player),

authenticating using customer triangle authentication,

transferring of all customer A play codes and play counts from the media ticket smart card A into the cryptographic digital signal processor including the customer A's private key and public key,

decrypting of customer A's play code and play count,

updating of vendor sequence number and customer (family key) sequence number,

committing 2-way operations of several cyclic loops from cryptographic digital signal processor to media ticket smart card and back again before finalising transaction computer operations,

permanently erasing in media ticket smart card A any removed play codes and play counts owned by customer A,

removing of the customer A's media ticket smart card from the cryptographic media player,

inserting of media ticket smart card B into the cryptographic digital signal processor (C-DSP) inside of a cryptographic media player (e.g. C-MP3 player),

authenticating using customer triangle authentication,

transferring of all customer B play codes and play counts from the media ticket smart card B into the cryptographic digital signal processor including the customer B's private key and public key,

decrypting of customer B's play code and play count,

creating a super-set list of play codes and play counts and re-encrypting them for customer B,

updating of vendor sequence number and customer (family key) sequence number,

transferring the super-set list of play codes and play counts back to media ticket smart card B for cryptographic storage,

committing 2-way operations of several cyclic loops from cryptographic digital signal processor to media ticket smart card and back again before finalising transaction computer operations,

permanently erasing all play codes and play counts of either party A or party B from the cryptographic media player,

removing of the customer B's media ticket smart card from the cryptographic media player,

25. The invention and components of claim 24 whereby the process of or method of steps to do legal archiving of custom encrypted digital media and also play code and play count ownership from media ticket smart A of owner A to back-up copies known as legal "fair use" under US Copyright law for means of archival storage in case of fire, theft, vandalism, storm, flooding, for a convenient home and car copy for marketing "fair use", which is accomplished by the sub-steps of:

copying of "cipher text (encrypted data)" digital media in digital to digital copying mode an unlimited number of times using a personal computer or other digital to digital copying device to create flawless digital archival copies which are usable only with media ticket smart card A primary card or media ticket smart card A back-up card,

updating of primary card to back-up card operations to allow both to be used for archival copy decryptions,

inserting of media ticket smart card A primary card into the cryptographic digital signal processor (C-DSP) inside of a cryptographic media player (e.g. C-MP3 player),

authenticating using customer triangle authentication,

transferring of all customer A primary card play codes and play counts from the media ticket smart card A into the

cryptographic digital signal processor including the customer A's private key and public key,

decrypting of customer A's primary card play code and play count,

updating of vendor sequence number and customer (family key) sequence number,

committing 2-way operations of several cyclic loops from cryptographic digital signal processor to media ticket smart card A primary card and back again before finalising transaction computer operations,

permanently erasing in media ticket smart card A primary card any removed play codes and play counts owned by customer A,

removing of the customer A's media ticket smart card primary card from the cryptographic media player,

inserting of media ticket smart card A back-up card into the cryptographic digital signal processor (C-DSP) inside of a cryptographic media player (e.g. C-MP3 player),

authenticating using customer triangle authentication,

transferring of all customer A back-up card play codes and play counts from the media ticket smart card A back-up card into

the cryptographic digital signal processor including the customer A's private key and public key,

decrypting of customer A's play code and play count,

creating a super-set list of play codes and play counts and re-encrypting them for customer A,

updating of vendor sequence number and customer (family key) sequence number,

transferring the super-set list of play codes and play counts back to media ticket smart card A back-up for cryptographic storage,

committing 2-way operations of several cyclic loops from cryptographic digital signal processor to media ticket smart card A back-up before finalising transaction computer operations,

removing of the customer A's media ticket smart card back-up from the cryptographic media player,

inserting of media ticket smart card A primary card again into the cryptographic digital signal processor (C-DSP) inside of a cryptographic media player (e.g. C-MP3 player),

authenticating using customer triangle authentication,

re-accessing in the cryptographic media player the already created super-set list of play codes and play counts and re-encrypting them for customer A,

updating vendor sequence number and customer (family key) sequence number,

transferring the super-set list of play codes and play counts back to media ticket smart card A back-up for cryptographic storage,

committing 2-way operations of several cyclic loops from cryptographic digital signal processor to media ticket smart card A back-up before finalising transaction computer operations,

permanently erasing all play codes and play counts of either party A primary card or party A back-up card from the cryptographic media player,

removing of the customer A's media ticket smart card primary from the cryptographic media player,

=====

26. A specific method of or process for doing public key cryptography over an open systems architecture in a totally cryptographically secure manner meant for safeguarding multi-million dollar digital masters which open systems architecture includes existing prior art components and some of the inventor's related new art invention components defined in his cross-reference to related inventions to give the systems components of:

computer hardware components (prior art):

tamper-resistant non-volatile memory used to hold embedded, cryptographic computer programs, cryptographic private keys, cryptographic secret keys, cryptographic session keys, and

often used cryptographic public keys (prior art),

random access memory (prior art),

micro-processors which have wiretappable buses and memory (prior art),

cryptographic embedded micro-processors containing tamper resistant non-volatile memory, random access memory, and embedded firmware for executing cryptographic algorithms over wiretappable

("red") buses and memory and non-wiretappable ("black") buses and cryptographic or secure memory and pass-thru encryption algorithms with means to get the secret data over wiretappable ("red") buses (prior art),

media ticket smart cards containing tamper resistant, non-volatile memory for key storage as part of cryptographic embedded micro-processors (prior art),

media ticket smart card readers containing embedded tamper resistant non-volatile memory for key storage as part of cryptographic embedded micro-processors (prior art),

local area networks (LAN's) (prior art),

internet protocol (IP) wide area networks (prior art),

world wide web (WWW) server computers (prior art),

personal computers (PC's) (prior art),

personal computer web clients (prior art),

personal computer peripherals (prior art),

cryptographic computer entry devices which include,

cryptographic toggle fields with visible mini-displays with a toggle field into which is entered a passphrase/passcode or in other words a condensed fixed alph-numeric pseudorandom mix of letters, numbers, and punctuation upon a cryptographic media

player device which contains a cryptographic digital signal processor,

cryptographic access codes which include passphrases/passcodes (prior art) typed into a computer keyboard (prior art),

bio-identification with first example means being a customer finger entered into a built-in digital fingerprint reader (prior art) to produce a digitized fingerprint,

personal computer peripheral data storage devices (prior art),
personal computer peripheral data storage media (prior art),

cryptographic hardware secret key algorithm sub-processors inside of cryptographic digital signal processors inside of cryptographic media players,

cryptographic computing units also called cryptographic media players which include:

cryptographic digital signal processors containing
cryptographic hardware secret key algorithm sub-processors,
tamper resistant non-volatile electrically erasable programmable read only memory, random access memory, analog to digital signal converters, moving picture electronics group hardware decompression circuitry for digital audio/video, digital audio/video signal artificial degradation circuitry, digital to analog signal converters, and digital signal processing of digital audio/video signals circuitry,

internal to a personal computer cryptographic media players which contain cryptographic digital signal processors and access through prior art personal computer peripherals to external prior art media ticket smart card readers and personal computer peripheral data storage media,

external to a personal computer cryptographic media players which contain cryptographic digital signal processors with built-in media ticket smart card readers and built-in personal computer peripheral data storage drives in first example means of a player being a cryptographic moving picture experts group standards I audio layer 3 or crypto-mp3 player,

cryptographic media players/high definition television broadcast receivers/cable digital signal receivers/embedded personal computer or smart set-top box/digital audio-video recorders which contain cryptographic digital signal processors with built-in media ticket smart card readers,

cryptographic media players/micro-mirror modules/theater projection/theater sound/digital versatile disk read/write drive units which contain cryptographic digital signal processorw with built-in media ticket smart card readers,

computer software components:

secure operating systems for world wide web server computers
(prior art),

world wide web cryptographic medium download programs (prior
art),

cryptographic mathematics algorithms:

public key cryptography algorithms which create public keys and
private keys, secret key cryptography algorithms which create secret
keys and session keys (1-time secret keys) and also play counts or
access counts or media decryption counts and play codes (session keys
or 1-time secret keys),

hybrid key cryptography algorithms which are combined public key
and private key cryptography algorithms (prior art),

private key and secret key splitting (prior art),

private key and secret key escrow (prior art),

cryptographic keys which are the collective public keys, private
keys, secret keys, session keys (1-time secret keys), play counts,
play codes, passphrases/passcodes (prior art),

computer cryptography protocols (prior art),

pass-thru encryption of cryptographic keys (prior art),

digital media formats (prior art),

computer communications protocols:

transmissions control protocol/internet protocol (TCP/IP) (prior art),

secure internet protocol layer (prior art),

secure sockets layer (prior art) (SSL),

world wide web server protocols such as hyper-text mark-up language (prior art) (HTML),

world wide web client protocols such as hyper-text mark-up language (prior art) (HTML),

and a specific new invention system process of or methods of public key cryptography comprising of the process steps of:

generating of system keys which is the process done by the media ticket smart card system authority's, party s's, dedicated public key

generation authority, party g, while having absolutely no access to customer identifications,

generating of media distribution vendor cryptographic keys eventually used in cryptographic digital signal processors for eventual manufacturing into cryptographic media players which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g, while having absolutely no access to customer identifications,

generating of media ticket smart card cryptographic keys which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g, while having absolutely no access to customer identifications,

distributing of cryptographic digital signal processors which is the process done by the media ticket smart card system authority's, party s's, dedicated public key distribution authority, party d, distributing cryptographic digital signal processors to media distribution vendors, parties vN, for manufacturing into cryptographic media players while having absolutely no access to whole cryptographic keys,

distributing of media ticket smart cards which is the process done by the media ticket smart card system authority's, party s's, dedicated public key distribution authority, party d, distributing media ticket smart cards to media distribution vendors for selling to customers while having absolutely no access to whole cryptographic keys,

layering for a federated cryptography architecture which is the process done by the media ticket smart card system authority, party s, creating a federated architecture of cryptographic authority with 3-layers, a central layer composed of the media ticket smart card system authority, a local layer composed of authorized media distribution companies vN, and a user layer composed of customers,

preparing of play codes and play counts which is the process done by the authorized digital media distribution company, party vN, preparing play codes (session keys or 1-time secret keys), play counts (paid for numbers of plays or counts of free trial plays), and custom encrypted digital media for downloading to each customer,

downloading to customer, party a, which is the process done by the authorized digital media distribution vendor, party vN, using hybrid key cryptographing steps of hybrid key cryptographic digital media distribution from a central media distribution authority hosted on a web server to multiple personal computer based web clients of encrypted play codes (1-time secret keys or session keys) with header and encrypted play counts (paid for counts of plays or decryptions, or else counts of free trial plays) with header for deposit into media ticket smart cards attached to personal computer media ticket smart card readers, and 1-way transfer of custom session key encrypted digital media for deposit into physical digital media inserted into media drives attached to personal computers,

delivering by foot which is the process done by the customer, party a, of physically transferring both physical custom encrypted digital

media and the customer, party a's, programmed media ticket smart cards from the customer's, party a's, personal computer to any person's cryptographic media player with a built-in media ticket smart card reader,

initializing before playing which is the process done by the customer, party a, of preparing any party's cryptographic media player with his own custom encrypted digital media his own media ticket smart card,

authenticating by customer triangle authentication which is the process done by the cryptographic digital signal processor embedded inside of a cryptographic media player,

transferring by pass-thru encryption of cryptographic keys which is the process done by the cryptographic media player to receive encrypted play codes with header and encrypted play counts with header from the media ticket smart card n transferred over wiretappable computer buses to the player's own cryptographic memory for access by its cryptographic digital signal processor,

transferring by pass-thru encryption of cryptographic keys which is the process done by the cryptographic media player's cryptographic digital signal processor to transfer encrypted play codes with header and encrypted play counts with header both with cryptographic digital signal processor incremented sequence counts to the media ticket smart card a transferred over wiretappable computer buses,

authenticating by media triangle authentication which is the process done by a cryptographic media player using digital media triangle authentication,

cryptographing using public key cryptography which is the process done by a cryptographic digital signal processor inside of a cryptographic media player using public key cryptography which is the process of using public key cryptography authentication, encryption, and decryption using public keys (puk-n), and private keys (prk-n), stored within tamper resistant non-volatile memory embedded within non-wiretappable ("black") cryptographic computing units in the example of cryptographic digital signal processors,

cryptographing using secret key cryptography which is the process done by a cryptographic digital signal processor inside of a cryptographic media player using secret key cryptography which is the process of using secret key cryptography with a non-wiretappable ("black") bus, cryptographic computing unit in example of a cryptographic digital signal processing unit using secret keys (sek-n), or session keys (ssk-n), stored upon tamper resistant, non-volatile memory,

cryptographing using fast hardware session key cryptography which is the process done by a cryptographic digital signal processor inside of a cryptographic media player using hardware secret key cryptography which is the process of using a dedicated hardware secret key sub-processor which is embedded within a secure ("black"), cryptographic digital signal processing unit with access to higher

level tamper resistant non-volatile ("black") memory for cryptographic key storage of private keys and secret keys, which hardware secret key sub-processor is much faster than software for secret key cryptography and is intended for fast, secret key cryptography encryption and decryption of block transferred digital media,

cryptographing using hybrid key cryptography which is the process done by a cryptographic digital signal processor inside of a cryptographic media player using hybrid key cryptography which is the process of using hybrid key cryptography which uses public key cryptography to authenticate remote parties, do digital signatures to authenticate digital media and establish media integrity with a remote party, and encrypt one-time secret keys known as session keys (ssk-n), used for only one session, which said session keys are sent to a remote party who decrypts them for storage in his own tamper resistant, non-volatile memory embedded on his black, cryptographic computing unit in the example of a cryptographic digital signal processor and a cryptographic central processing unit which said session keys may be later stored in tamper resistant non-volatile memory embedded in a media ticket smart card where they are referred to as play codes with paid for and authorized play counts.

accounting by the cryptographic digital signal processor which is the process done by the cryptographic media player using hybrid key cryptography digital media playing of 1-way transfer of custom session key encrypted digital media owned by party n in a controlled access manner mostly for financial accounting purposes which uses the

play codes (session key or 1-time secret key) and play counts (paid for number of plays or count of free trial plays) contained in media ticket smart cards,

playing by the cryptographic digital signal processor which is the process done by the cryptographic media player using hybrid key cryptography which is the process of using hybrid key cryptography to do digital media playing in a controlled access manner using play codes (session key or 1-time secret keys) and play counts (now contained within registers in the cryptographic digital signal processor and also the hardware secret key decryption device directly used upon the custom encrypted 1-way transfer of custom session key encrypted digital media,

escrowing retrieval of lost, stolen, or disputed ownership media ticket smart cards which is the process done by the customer, party n, which collection of processes of or methods of invention sets systems standards and integrates components into a system which can be used in the future for new forms of internationally standardized cryptography sanctioned by industry tradegroups such as the Recording Industry of America Association (RIAA), the Secure Digital Music Initiative (SDMI), the US National Association of Broadcasters (NAB), and also national standards agencies such as the American National Standards Institute (ANSI), National Institute for Standards and Technology (NIST), or International Telegraphy Union (ITU).

=====

27. A specific method of or process for doing public key cryptography over an open systems architecture in a totally cryptographically secure manner meant for safeguarding multi-million dollar digital masters for the specific process of "over the air," broadband cable, broadband phone line, direct digital satellite, or Institute of Electrical and Electronic Engineers (IEEE 802.11c) wireless Ethernet distribution of custom pre-encrypted, "cipher text," digital media in high definition television (HDTV)/standards definition television (SDTV) digital form which open systems architecture includes existing prior art components and some related new art inventions developed by the inventor defined in his cross-reference to related inventions to give the systems components of:

computer hardware components:

tamper-resistant non-volatile memory used to hold embedded, cryptographic computer programs, cryptographic private keys, cryptographic secret keys, cryptographic session keys, and

often used cryptographic public keys (prior art),

random access memory (prior art),

micro-processors which have wiretappable buses and memory (prior art),

cryptographic embedded micro-processors containing tamper resistant non-volatile electrically erasable programmable read only memory (TNV-EEPROM), random access memory (RAM), and embedded firmware for executing cryptographic algorithms over wiretappable ("red") buses and memory and non-wiretappable ("black") buses and cryptographic or secure memory and pass-thru encryption algorithms with means to get the secret data over wiretappable ("red") buses (prior art),

media ticket smart cards containing tamper resistant, non-volatile memory for key storage as part of cryptographic embedded micro-processors (prior art),

media ticket smart card readers containing embedded tamper resistant non-volatile memory for key storage as part of cryptographic embedded micro-processors (prior art),

local area networks (prior art),

internet protocol wide area networks (prior art),

world wide web server computers (prior art),

personal computers (prior art),

personal computer web clients (prior art),

personal computer peripherals (prior art),

cryptographic computer entry devices which include,

cryptographic toggle fields with visible mini-displays with a toggle field into which is entered a passphrase/passcode or in other words a condensed fixed alph-numeric pseudorandom mix of letters, numbers, and punctuation upon a cryptographic media player device which contains a cryptographic digital signal processor,

cryptographic access codes which include
passphrases/passcodes (prior art) typed into a computer keyboard (prior art),

bio-identification with first example means being a customer finger entered into a built-in digital fingerprint reader (prior art) to produce a digitized fingerprint,

personal computer peripheral data storage devices (prior art),

personal computer peripheral data storage media (prior art),

cryptographic hardware secret key algorithm sub-processors inside of cryptographic digital signal processors inside of cryptographic media players,

cryptographic computing units also called cryptographic set-top boxes with computer monitors and also built-in set-top boxes in digital televisions which include:

cryptographic digital signal processors containing cryptographic hardware secret key algorithm sub-processors, tamper resistant non-volatile electrically erasable programmable read only memory, random access memory, analog to digital signal converters, moving picture electronics group hardware decompression circuitry for digital audio/video, digital audio/video signal artificial degradation circuitry, digital to analog signal converters, and digital signal processing of digital audio/video signals circuitry,

internal to a personal computer cryptographic media players which contain cryptographic digital signal processors and access through prior art personal computer peripherals to external prior art media ticket smart card readers and personal computer peripheral data storage media,

external to a personal computer cryptographic media players which contain cryptographic digital signal processors with built-in media ticket smart card readers and built-in personal computer peripheral data storage drives in example means of a player being a cryptographic moving picture experts group standards I audio layer 3 or crypto-mp3 player,

cryptographic media players called set-top boxes with a digital television monitor and also built-in a digital

television which can receive "over the air" digital signals, direct satellite signals, broadband cable signals, broadband ADSL phone signals, or IEEE 802.11c wireless Ethernet signals all in custom, pre-encrypted, "cipher-text," high definition television (HDTV) or standard definition broadcast (SDTV) form to digital signal receivers, digital tuners, and cryptographic digital signal processors with built-in media ticket smart card readers,

cryptographic media players/micro-mirror modules/theater projection/theater sound/digital versatile disk read/write drive units which contain cryptographic digital signal processorw with built-in media ticket smart card readers,

computer software components:

secure operating systems for world wide web server computers (prior art),

world wide web cryptographic medium download programs (prior art),

cryptographic mathematics algorithms:

public key cryptography algorithms which create public keys and private keys, secret key cryptography algorithms which create secret keys and session keys (1-time secret keys) and also play counts or access counts or media decryption counts and play codes (session keys or 1-time secret keys),

hybrid key cryptography algorithms which are combined public key and private key cryptography algorithms (prior art),

private key and secret key splitting (prior art),

private key and secret key escrow (prior art),

cryptographic keys which are the collective public keys, private keys, secret keys, session keys (1-time secret keys), play counts, play codes, passphrases/passcodes (prior art),

computer cryptography protocols (prior art),

pass-thru encryption of cryptographic keys (prior art),

digital media formats (prior art),

computer communications protocols:

transmissions control protocol/internet protocol (prior art)
(TCP/IP),

secure internet protocol layer (prior art),

secure sockets layer (prior art) (SSL),

world wide web server protocols such as hyper-text mark-up
language (prior art) (HTML),

world wide web client protocols such as hyper-text mark-up
language (prior art) (HTML),

and a specific new invention system process of or methods of public key
cryptography comprising of the process steps of:

generating of system keys which is the process done by the media
ticket smart card system authority's, party s's, dedicated public
key generation authority, party g, while having absolutely no
access to customer identifications,

generating of media distribution vendor cryptographic keys
eventually used in cryptographic digital signal processors for
eventual manufacturing into cryptographic media players which is
the process done by the media ticket smart card system authority's,

party s's, dedicated public key generation authority, party g, while having absolutely no access to customer identifications,

generating of media ticket smart card cryptographic keys which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g, while having absolutely no access to customer identifications,

distributing of cryptographic digital signal processors which is the process done by the media ticket smart card system authority's, party s's, dedicated public key distribution authority, party d, distributing cryptographic digital signal processors to media distribution vendors, parties vN, for manufacturing into cryptographic media players called set-top boxes while having absolutely no access to whole cryptographic keys,

distributing of media ticket smart cards which is the process done by the media ticket smart card system authority's, party s's, dedicated public key distribution authority, party d, distributing media ticket smart cards to media distribution vendors for selling to customers while having absolutely no access to whole cryptographic keys,

layering for a federated cryptography architecture which is the process done by the media ticket smart card system authority, party s, creating a federated architecture of cryptographic authority with 3-layers, a central layer composed of the media ticket smart

card system authority, a local layer composed of authorized media distribution companies vN, and a user layer composed of customers,

preparing of play codes and play counts which is the process done by the authorized digital media distribution company, party vN, preparing play codes (session keys or 1-time secret keys), play counts (paid for numbers of plays or counts of free trial plays), and custom encrypted digital media for downloading to each customer,

downloading to customer, party a, which is the process done by the authorized digital media distribution vendor, party vN, using hybrid key cryptographing steps of hybrid key cryptographic digital media distribution from a central media distribution authority hosted on a web server to multiple personal computer based web clients of encrypted play codes (1-time secret keys or session keys) with header and encrypted play counts (paid for counts of plays or decryptions, or else counts of free trial plays) with header for deposit into media ticket smart cards attached to personal computer media ticket smart card readers, and 1-way transfer of custom session key encrypted digital media for deposit into physical digital media inserted into media drives attached to personal computers,

delivering by foot which is the process done by the customer, party a, of physically transferring a programmed media ticket smart card from the customer's, party a's, personal computer to any

person's cryptographic media player with a built-in media ticket smart card reader,

custom broadcasting to customer, party a, which is the process done by the authorized digital media distribution vendor, party vN, using hybrid key cryptographic steps of hybrid key cryptographic digital media distribution from a central media distribution authority hosted on a broadcast server to multiple homes or businesses having cryptographic set-top boxes for 1-way transfer of custom session key encrypted digital media for possible digital recording into physical digital media inserted into media drives attached to an attached digital recorder,

initializing before playing which is the process done by the customer, party a, of preparing any party's cryptographic set-top box for his own custom broadcast encrypted digital media and his own media ticket smart card,

authenticating by customer triangle authentication which is the process done by the cryptographic digital signal processor embedded inside of a cryptographic set-top box,

transferring by pass-thru encryption of cryptographic keys which is the process done by the cryptographic set-top box to receive encrypted play codes with header and encrypted play counts with header from the media ticket smart card n transferred over wiretappable computer buses to the set-top box's own cryptographic memory for access by its cryptographic digital signal processor,

transferring by pass-thru encryption of cryptographic keys which is the process done by the cryptographic set-top box's cryptographic digital signal processor to transfer encrypted play codes with header and encrypted play counts with header both with cryptographic digital signal processor incremented sequence counts to the media ticket smart card a transferred over wiretappable computer buses,

authenticating by media triangle authentication which is the process done by a cryptographic set-top box using digital media triangle authentication,

cryptographing using public key cryptography which is the process done by a cryptographic digital signal processor inside of a cryptographic set-top box using public key cryptography which is the process of using public key cryptography authentication, encryption, and decryption using public keys (puk-n), and private keys (prk-n), stored within tamper resistant non-volatile memory embedded within non-wiretappable ("black") cryptographic computing units in the example of cryptographic digital signal processors,

cryptographing using secret key cryptography which is the process done by a cryptographic digital signal processor inside of a cryptographic set-top box using secret key cryptography which is the process of using secret key cryptography with a non-wiretappable ("black") bus, cryptographic computing unit in example of a cryptographic digital signal processing unit using secret keys

(sek-n), or session keys (ssk-n), stored upon tamper resistant, non-volatile memory,

cryptographing using fast hardware session key cryptography which is the process done by a cryptographic digital signal processor inside of a cryptographic set-top box using hardware secret key cryptography which is the process of using a dedicated hardware secret key sub-processor which is embedded within a secure ("black"), cryptographic digital signal processing unit with access to higher level tamper resistant non-volatile ("black") memory for cryptographic key storage of private keys and secret keys, which hardware secret key sub-processor is much faster than software for secret key cryptography and is intended for fast, secret key cryptography encryption and decryption of block transferred digital media,

cryptographing using hybrid key cryptography which is the process done by a cryptographic digital signal processor inside of a cryptographic set-top box using hybrid key cryptography which is the process of using hybrid key cryptography which uses public key cryptography to authenticate remote parties, do digital signatures to authenticate digital media and establish media integrity with a remote party, and encrypt one-time secret keys known as session keys (ssk-n), used for only one session, which said session keys are sent to a remote party who decrypts them for storage in his own tamper resistant, non-volatile memory embedded on his black, cryptographic computing unit in the example of a cryptographic digital signal processor and a cryptographic central processing

unit which said session keys may be later stored in tamper resistant non-volatile memory embedded in a media ticket smart card where they are referred to as play codes with paid for and authorized play counts.

accounting by the cryptographic digital signal processor which is the process done by the cryptographic set-top box using hybrid key cryptography digital media playing of 1-way transfer of custom session key encrypted digital media owned by party n in a controlled access manner mostly for financial accounting purposes which uses the play codes (session key or 1-time secret key) and play counts (paid for number of plays or count of free trial plays) contained in media ticket smart cards,

playing by the cryptographic digital signal processor which is the process done by the cryptographic set-top box using hybrid key cryptography which is the process of using hybrid key cryptography to do digital media playing in a controlled access manner using play codes (session key or 1-time secret keys) and play counts (now contained within registers in the cryptographic digital signal processor and also the hardware secret key decryption device directly used upon the custom encrypted 1-way transfer of custom session key encrypted digital media,

electronic television guide picture in a picture (PIP) viewing and channel selection and future program recording such as through an example graphical user interface (GUI) means of a "spreadsheet type" or "matrix type" of display accomplished through a process

new with the inventor's cross referenced invention [REF 512] which uses a new cryptography "silhouette-like" technique extension to the MPEG IV standards for very efficient carrying of limited digital television guide information which can easily be removed in a MPEG X decompression circuit for sending to video RAM and subsequent display in a digital picture in a picture (PIP) on a digital monitor,

escrowing retrieval of lost, stolen, or disputed ownership media ticket smart cards which is the process done by the customer, party n, which collection of processes of or methods of invention sets systems standards and integrates components into a system which can be used in the future for new forms of internationally standardized cryptography sanctioned by industry tradegroups such as the Recording Industry of America Association (RIAA), the Secure Digital Music Initiative (SDMI), the US National Association of Broadcasters (NAB), and also national standards agencies such as the American National Standards Institute (ANSI), National Institute for Standards and Technology (NIST), or International Telegraphy Union (ITU).

=====

28. A specific method of or process for doing public key cryptography over an open systems architecture in a totally cryptographically secure manner meant for safeguarding multi-million dollar digital masters for the process of commercial movie distribution involving fully digital micro-mirror modules (MMM) which open systems architecture includes existing prior art components and some related new art inventions developed by the inventor and defined in the cross-reference to the inventor's patents to give the systems components of:

computer hardware components:

tamper-resistant non-volatile memory used to hold embedded, cryptographic computer programs, cryptographic private keys, cryptographic secret keys, cryptographic session keys, and

often used cryptographic public keys (prior art),

random access memory (prior art),

micro-processors which have wiretappable buses and memory (prior art),

cryptographic embedded micro-processors containing tamper resistant non-volatile memory, random access memory, and embedded firmware for

executing cryptographic algorithms over wiretappable ("red") buses and memory and non-wiretappable ("black") buses and cryptographic or secure memory and pass-thru encryption algorithms with means to get the secret data over wiretappable ("red") buses (prior art),

media ticket smart cards containing tamper resistant, non-volatile memory for key storage as part of cryptographic embedded micro-processors (prior art),

media ticket smart card readers containing embedded tamper resistant non-volatile memory for key storage as part of cryptographic embedded micro-processors (prior art),

local area networks (prior art),

internet protocol wide area networks (prior art),

world wide web server computers (prior art),

personal computers (prior art),

personal computer web clients (prior art),

personal computer peripherals (prior art),

cryptographic computer entry devices which include,

cryptographic toggle fields with visible mini-displays with a toggle field into which is entered a passphrase or in other words a short alpha-numeric sentence with punctuation or a passcode or in other words a condensed fixed alpha-numeric pseudorandom mix of

letters, numbers, and punctuation with no vowels upon a cryptographic media player device which contains a cryptographic digital signal processor,

cryptographic access codes which include passphrases and passcodes (prior art) typed into a computer keyboard (prior art),

bio-identification with first example means being a customer finger entered into a built-in digital fingerprint reader (prior art) to produce a digitized fingerprint,

personal computer peripheral data storage devices (prior art),
personal computer peripheral data storage media (prior art),

cryptographic hardware secret key algorithm sub-processors inside of cryptographic digital signal processors inside of cryptographic media players,

cryptographic computing units also called cryptographic media players which include:

cryptographic digital signal processors containing cryptographic hardware secret key algorithm sub-processors, tamper resistant non-volatile electrically erasable programmable read only memory, random access memory, analog to digital signal converters, moving picture electronics group hardware decompression circuitry for digital audio/video, digital audio/video signal artificial degradation circuitry, digital to analog signal converters, and digital signal processing of digital audio/video signals circuitry,

internal to a personal computer cryptographic media players which contain cryptographic digital signal processors and access through prior art personal computer peripherals to external prior art media ticket smart card readers and personal computer peripheral data storage media,

external to a personal computer cryptographic media players which contain cryptographic digital signal processors with built-in media ticket smart card readers and built-in personal computer peripheral data storage drives in first example means of a player being a cryptographic moving picture experts group standards I audio layer 3 or crypto-mp3 player,

cryptographic media players/high definition television broadcast receivers/cable digital signal receivers/embedded personal computer or smart set-top box/digital audio-video recorders which contain cryptographic digital signal processors with built-in media ticket smart card readers,

cryptographic media players/micro-mirror modules/theater projection/theater sound/digital versatile disk read/write drive units which contain cryptographic digital signal processors with built-in media ticket smart card readers,

computer software components:

secure operating systems for world wide web server computers (prior art),

world wide web cryptographic medium download programs (prior art),

cryptographic mathematics algorithms:

public key cryptography algorithms which create public keys and private keys, secret key cryptography algorithms which create secret keys and session keys (1-time secret keys) and also play counts or access counts or media decryption counts and play codes (session keys or 1-time secret keys),

hybrid key cryptography algorithms which are combined public key and private key cryptography algorithms (prior art),

private key and secret key splitting (prior art),

private key and secret key escrow (prior art),

cryptographic keys which are the collective public keys, private keys, secret keys, session keys (1-time secret keys), play counts, play codes, passphrases, and passcodes (prior art),

computer cryptography protocols (prior art),

pass-thru encryption of cryptographic keys (prior art),

digital media formats (prior art),

computer communications protocols:

transmissions control protocol/internet protocol (prior art)
(TCP/IP),

secure internet protocol layer (prior art),

secure sockets layer (prior art) (SSL),

world wide web server protocols such as hyper-text mark-up
language (prior art) (HTML),

world wide web client protocols such as hyper-text mark-up
language (prior art) (HTML),

and a specific new invention system process of or methods of public key
cryptography comprising of the steps of:

generating of system keys which is the process done by the media
ticket smart card system authority's, party s's, dedicated public key
generation authority, party g, while having absolutely no access to
customer identifications,

generating of media distribution vendor cryptographic keys eventually used in cryptographic digital signal processors for eventual manufacturing into cryptographic micro mirror modules which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g, while having absolutely no access to customer identifications,

generating of media ticket smart card cryptographic keys which is the process done by the media ticket smart card system authority's, party s's, dedicated public key generation authority, party g, while having absolutely no access to customer identifications,

distributing of cryptographic digital signal processors which is the process done by the media ticket smart card system authority's, party s's, dedicated public key distribution authority, party d, distributing cryptographic digital signal processors to media distribution vendors, parties vN, for manufacturing into cryptographic micro-mirror module players while having absolutely no access to whole cryptographic keys,

distributing of media ticket smart cards which is the process done by the media ticket smart card system authority's, party s's, dedicated public key distribution authority, party d, distributing media ticket smart cards to media distribution vendors for selling to customers while having absolutely no access to whole cryptographic keys,

layering for a federated cryptography architecture which is the process done by the media ticket smart card system authority, party s, creating a federated architecture of cryptographic authority with 3-layers, a central layer composed of the media ticket smart card system

authority, a local layer composed of authorized media distribution companies vN, and a user layer composed of customers,

preparing of play codes and play counts which is the process done by the authorized digital media distribution company, party vN, preparing play codes (session keys or 1-time secret keys), play counts (paid for numbers of plays or counts of free trial plays), and custom encrypted digital media for downloading to each customer,

downloading to customer, party a, which is the process done by the authorized digital media distribution vendor, party vN, using hybrid key cryptographing steps of hybrid key cryptographic digital media distribution from a central media distribution authority hosted on a web server to multiple personal computer based web clients of encrypted play codes (1-time secret keys or session keys) with header and encrypted play counts (paid for counts of plays or decryptions, or else counts of free trial plays) with header for deposit into media ticket smart cards attached to personal computer media ticket smart card readers, and 1-way transfer of custom session key encrypted digital media for deposit into physical digital media inserted into media drives attached to personal computers,

delivering by foot which is the process done by the customer, party a, of physically transferring both physical custom encrypted digital media and the customer, party a's, programmed media ticket smart cards from the customer's, party a's, personal computer to any person's cryptographic micro mirror module with a built-in media ticket smart card reader,

initializing before playing which is the process done by the customer, party a, of preparing any party's cryptographic micro mirror module with his own custom encrypted digital media movies and his own media ticket smart card,

authenticating by customer triangle authentication which is the process done by the cryptographic digital signal processor embedded inside of a cryptographic micro mirror module,

transferring by pass-thru encryption of cryptographic keys which is the process done by the cryptographic micro mirror module to receive encrypted play codes with header and encrypted play counts with header from the media ticket smart card n transferred over wiretappable computer buses to the cryptographic micro mirror module's own cryptographic memory for access by its cryptographic digital signal processor,

transferring by pass-thru encryption of cryptographic keys which is the process done by the cryptographic media player's cryptographic micro mirror module to transfer encrypted play codes with header and encrypted play counts with header both with cryptographic digital signal processor incremented sequence counts to the media ticket smart card a transferred over wiretappable computer buses,

authenticating by media triangle authentication which is the process done by a cryptographic micro mirror module using digital media triangle authentication,

cryptographing using public key cryptography which is the process done by a cryptographic digital signal processor inside of a cryptographic micro mirror module using public key cryptography which is the process of using public key cryptography authentication, encryption, and decryption using public keys (puk-n), and private keys (prk-n), stored within tamper resistant non-volatile memory embedded within non-wiretappable ("black") cryptographic computing units in the example of cryptographic digital signal processors,

cryptographing using secret key cryptography which is the process done by a cryptographic digital signal processor inside of a cryptographic micro mirror module using secret key cryptography which is the process of using secret key cryptography with a non-wiretappable ("black") bus, cryptographic computing unit in example of a cryptographic digital signal processing unit using secret keys (sek-n), or session keys (ssk-n), stored upon tamper resistant, non-volatile memory,

cryptographing using fast hardware session key cryptography which is the process done by a cryptographic digital signal processor inside of a cryptographic micro mirror module using hardware secret key cryptography which is the process of using a dedicated hardware secret key sub-processor which is embedded within a secure ("black"), cryptographic digital signal processing (C-DSP) unit with access to higher level tamper resistant non-volatile ("black") memory for cryptographic key storage of private keys and secret keys, which hardware secret key sub-processor is much faster than software for secret key cryptography and is intended for fast, secret key

cryptography encryption and decryption of block transferred digital media,

cryptographing using hybrid key cryptography which is the process done by a cryptographic digital signal processor (C-DSP) inside of a cryptographic micro mirror module using hybrid key cryptography which is the process of using hybrid key cryptography which uses public key cryptography to authenticate remote parties, do digital signatures to authenticate digital media and establish media integrity with a remote party, and encrypt one-time secret keys known as session keys (ssk-n), used for only one session, which said session keys are sent to a remote party who decrypts them for storage in his own tamper resistant, non-volatile memory embedded on his black, cryptographic computing unit in the example of a cryptographic digital signal processor and a cryptographic central processing unit which said session keys may be later stored in tamper resistant non-volatile memory embedded in a media ticket smart card where they are referred to as play codes with paid for and authorized play counts.

accounting by the cryptographic digital signal processor which is the process done by the cryptographic micro mirror module using hybrid key cryptography digital media playing of 1-way transfer of custom session key encrypted digital media owned by party n in a controlled access manner mostly for financial accounting purposes which uses the play codes (session key or 1-time secret key) and play counts (paid for number of plays or count of free trial plays) contained in media ticket smart cards,

playing by the cryptographic digital signal processor which is the process done by the cryptographic micro-mirror module player using hybrid key cryptography which is the process of using hybrid key cryptography to do digital media playing in a controlled access manner using play codes (session key or 1-time secret keys) and play counts (now contained within registers in the cryptographic digital signal processor and also the hardware secret key decryption device directly used upon the custom encrypted 1-way transfer of custom session key encrypted digital media,

escrowing retrieval of lost, stolen, or disputed ownership media ticket smart cards which is the process done by the customer, party n, which collection of processes or methods of invention sets systems standards and integrates components into a system which can be used in the future for new forms of internationally standardized cryptography sanctioned by industry tradegroups such as the Recording Industry of America Association (RIAA), the Secure Digital Music Initiative (SDMI), the US National Association of Broadcasters (NAB), and also national standards agencies such as the American National Standards Institute (ANSI), National Institute for Standards and Technology (NIST), or International Telegraphy Union (ITU).

DRAWINGS:

See attached.